

ASG-PreAlert[®] IDMS/MVS System Guide

Version 4.3

Publication Number: PAC1400-43

Publication Date: June 2001

The information contained herein is the confidential and proprietary information of Allen Systems Group, Inc. Unauthorized use of this information and disclosure to third parties is expressly prohibited. This technical publication may not be reproduced in whole or in part, by any means, without the express written consent of Allen Systems Group, Inc.

© 1995-2001 Allen Systems Group, Inc. All rights reserved.
All names and products contained herein are the trademarks or registered trademarks of their respective holders.

ASG Documentation/Product Enhancement Fax Form

Please FAX comments regarding ASG products and/or documentation to (941) 263-3692.

Company Name	Telephone Number	Site ID	Contact name

Product Name/Publication	Version #	Publication Date
Product:		
Publication:		
Tape VOLSER:		

Enhancement Request:

ASG Support Numbers

ASG provides support throughout the world to resolve questions or problems regarding installation, operation, or use of our products. We provide all levels of support during normal business hours and emergency support during non-business hours. To expedite response time, please follow these procedures.

Please have this information ready:

- Product name, version number, and release number
- List of any fixes currently applied
- Any alphanumeric error codes or messages written precisely or displayed
- A description of the specific steps that immediately preceded the problem
- The severity code (ASG Support uses an escalated severity system to prioritize service to our clients. The severity codes and their meanings are listed below.)

If You Receive a Voice Mail Message:

- 1** Follow the instructions to report a production-down or critical problem.
- 2** Leave a detailed message including your name and phone number. A Support representative will be paged and will return your call as soon as possible.
- 3** Please have the information described above ready for when you are contacted by the Support representative.

Severity Codes and Expected Support Response Times

Severity	Meaning	Expected Support Response Time
1	Production down, critical situation	Within 30 minutes
2	Major component of product disabled	Within 2 hours
3	Problem with the product, but customer has work-around solution	Within 4 hours
4	"How-to" questions and enhancement requests	Within 4 hours

ASG provides software products that run in a number of third-party vendor environments. Support for all non-ASG products is the responsibility of the respective vendor. In the event a vendor discontinues support for a hardware and/or software product, ASG cannot be held responsible for problems arising from the use of that unsupported version.

Business Hours Support

Your Location	Phone	Fax	E-mail
United States and Canada	800.354.3578 1.941.435.2201 Secondary Numbers: 800.227.7774 800.525.7775	941.263.2883	support@asg.com
Australia	61.2.9460.0411	61.2.9460.0280	support.au@asg.com
England	44.1727.736305	44.1727.812018	support.uk@asg.com
France	33.141.028590	33.141.028589	support.fr@asg.com
Germany	49.89.45716.300	49.89.45716.400	support.de@asg.com
Singapore	65.224.3080	65.224.8516	support.sg@asg.com
All other countries:	1.941.435.2201		support@asg.com

Non-Business Hours - Emergency Support

Your Location	Phone	Your Location	Phone
United States and Canada	800.354.3578 1.941.435.2201 Secondary Numbers: 800.227.7774 800.525.7775 Fax: 941.263.2883		
Asia	011.65.224.3080	Japan/Telecom	0041.800.9932.5536
Australia	0011.800.9932.5536	New Zealand	00.800.9932.5536
Denmark	00.800.9932.5536	South Korea	001.800.9932.5536
France	00.800.9932.5536	Sweden/Telia	009.800.9932.5536
Germany	00.800.9932.5536	Switzerland	00.800.9932.5536
Hong Kong	001.800.9932.5536	Thailand	001.800.9932.5536
Ireland	00.800.9932.5536	United Kingdom	00.800.9932.5536
Israel/Bezeq	014.800.9932.5536		
Japan/IDC	0061.800.9932.5536	All other countries	1.941.435.2201

ASG Web Site

Visit <http://www.asg.com>, ASG's World Wide Web site.

Submit all product and documentation suggestions to ASG's product management team at <http://www.asg.com/products/suggestions.asp>

If you do not have access to the web, FAX your suggestions to product management at (941) 263-3692. Please include your name, company, work phone, e-mail ID, and the name of the ASG product you are using. For documentation suggestions include the publication number located on the publication's front cover.

Contents

Preface	v
About This Publication	v
Related Publications	vi
Publication Conventions	vi
1 Introduction	1
PreAlert Multiple User Sessions	1
2 Installing PreAlert	3
Installation Checklist	4
Step 1 - Installing PreAlert/TSO	8
1.1 Unloading Installation JCL	8
1.2 Unloading Installation Tape	9
1.3 Applying PreAlert Product Authorization and Maintenance	9
1.4 Specifying Userdata Options	10
1.5 Authorizing PreAlert	12
1.6 Initializing Statistics Logging	14
1.7 Starting PreAlert	16
1.8 Logging on to PreAlert/TSO	17
1.9 Using the PreAlert/TSO ISPF Interface	19
Step 2 - Installing PreAlert/VTAM	21
2.1 Verifying PreAlert/TSO Installation	21
2.2 Defining the VTAM Application ID	21
2.3 Authorizing PreAlert	22
2.4 Assessing Link Library Authorizations	22
2.5 Setting Security	22
2.6 Specifying Userdata Options	22
2.7 Starting PreAlert	23
2.8 Log on to PreAlert/VTAM	24
2.9 Utilizing Extended Features	26
Step 3 - Installing PreAlert/Local TSO	31

3.1 Adding TSO Authorized Program List	31
3.2 Using PreAlert/Local TSO	31
3 PreAlert Messages and Codes.....	33
PreAlert Started Task Messages	33
PreAlert Abend Codes	38
PreAlert Abend Summary	38
PreAlert User Abend Codes	39
Authorization Messages	40
4 Userdata Macros	41
UDPARMS PreAlert User Installation Data	42
UDPARMS Macro Example for PreAlert/TSO Userdata Options	42
UDPARMS Macro Example for PreAlert/VTAM Userdata Options	43
UDPARMS Option Cross-reference	43
UDPARMS Option Descriptions	48
User Authorization and Security Options	48
Print Options	51
Message Options	51
Statistics Logging Options	51
Color/Highlighting Options	52
Miscellaneous Options (of General Scope)	53
IDMS Options	55
ASG-SIRF Options	58
MVS Options	58
VTAM Options	59
TSO Options	60
ASG-SERVER FACILITY Options	61
UDAUSER Authorized User IDs	61
UDLCX Line Command Exclude Feature	62
UDPGN MVS Performance Group Names	63
UDDOM MVS Domain Names	64
UDEXAL MVS Exception Analysis Default Level Sets	65
UDCVNUM IDMS/CV Numbers	66
UDIJOBS IDMS Jobname Lists	66
UDIJOBS Macro Options	67
UDIDXl IDMS Exception Analysis Default Level	67

5	Security Considerations	69
	Default Security Features	70
	Line Command Exclude Feature	71
	Security Exit	72
	Sample Security Exits	74
	Secured Line Commands and Functions	77
	IDMS Interface	77
	Storage Display and Modification	77
	Master Console Support	78
	MVS System Services	78
	Dataset Displays	79
	Address Space Restricted Functions	79
	Control Commands	79
	MVS Wait Analysis	79
	Authorized User IDs	80
	SMF Logging	80
	AMVS Security Facility	80
	AMVS Secured Functions	81
	Index	83

Preface

This *ASG-PreAlert IDMS/MVS System Guide* provides ASG-PreAlert (herein called PreAlert) reference information and an installation checklist, as well as installation instructions and a description of security considerations.

Allen Systems Group, Inc. (ASG) provides professional support to resolve any questions or concerns regarding the installation or use of any ASG product. Telephone technical support is available around the world, 24 hours a day, 7 days a week.

ASG welcomes your comments, as a preferred or prospective customer, on this publication or on any ASG product.

About This Publication

This publication consists of these chapters:

- [Chapter 1, "Introduction,"](#) introduces the reader to PreAlert.
- [Chapter 2, "Installing PreAlert,"](#) describes the installation procedures in a step-by-step method.
- [Chapter 3, "PreAlert Messages and Codes,"](#) delineates PreAlert's started task messages,abend codes and summary, and authorization messages.
- [Chapter 4, "Userdata Macros,"](#) explains the userdata macros that are available to your site with the PreAlert product.
- [Chapter 5, "Security Considerations,"](#) discusses the security features of PreAlert, providing samples of the security exits and secured line command information.

Related Publications

The complete documentation library for ASG-PreAlert consists of these publications (where *nn* represents the product version number):

- *ASG-PreAlert IDMS/MVS System Guide* (PAC1400-*nn*) provides information regarding PreAlert realtime operating system.
- *ASG-PreAlert IDMS User's Guide* (PAI0200-*nn*) provides complete instructions on how to use PreAlert for performing realtime IDMS system monitoring.
- *ASG-PreAlert MVS User's Guide* (PAM0200-*nn*) describes the functions and operations of PreAlert as a monitor and control system in the MVS environment.
- *ASG-PreAlert MSP System Guide* (PAF1400-*nn*-MSP) describes the codes and abends useful to operating ASG-PreAlert MSP.
- *ASG-PreAlert MSP User's Guide* (PAF0200-*nn*-MSP) provides complete instructions on how to use ASG-PreAlert MSP for performing realtime MSP system monitoring.

Note: _____

To obtain a specific version of a publication, contact the ASG Service Desk.

Publication Conventions

ASG uses these conventions in technical publications:

Convention	Represents
ALL CAPITALS	Directory, path, file, dataset, member, database, program, command, and parameter names.
Initial Capitals on Each Word	Window, field, field group, check box, button, panel (or screen), option names, and names of keys. A plus sign (+) is inserted for key combinations (e.g., Alt+Tab).
<i>lowercase italic monospace</i>	Information that you provide according to your particular situation. For example, you would replace <i>filename</i> with the actual name of the file.
Monospace	Characters you must type exactly as they are shown. Code, JCL, file listings, or command/statement syntax. Also used for denoting brief examples in a paragraph.
Vertical Separator Bar () with underline	Options available with the default value underlined (e.g., Y <u>N</u>).

1

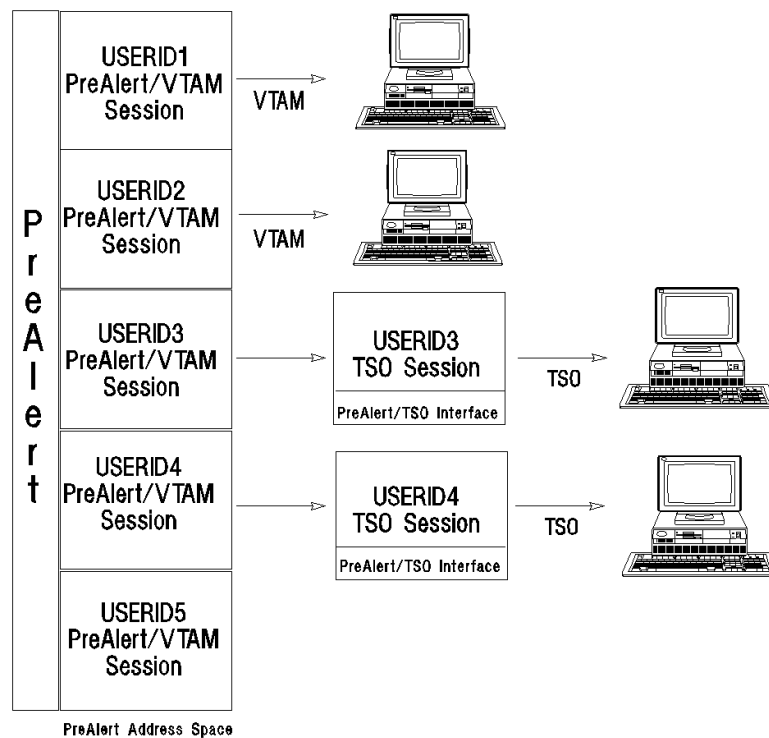
Introduction

PreAlert is a realtime control system which targets and corrects problems across single or multiple central versions (CVs), or single or multiple address spaces, thus enhancing management and control of your IDMS processing environment.

PreAlert Multiple User Sessions

[Figure 1](#) represents a typical PreAlert multi-user session with five user sessions active in the PreAlert Address Space.

Figure 1 • PreAlert multi-user session



USERID1 and USERID2 use the PreAlert/VTAM interface. In the VTAM interface, the sessions use VTAM macros to send and receive data to and from the terminal.

USERID3 and USERID4 use the PreAlert/TSO interface. When the TSO interface is used, all data collection and analysis are done in the PreAlert address space, and screen images are then placed in extended CSA. The PreAlert/TSO interface executing in the user's TSO address space takes the data from CSA and uses TSO TGET and TPUT macros to communicate with the terminal.

USERID5 uses a PreAlert background session. In a background session, all terminal input and output is suppressed, but the session continues just as if a terminal were attached. The user can log on to the session via either the VTAM interface or TSO interface.

2

Installing PreAlert

This chapter covers these topics:

Overview	4
Installation Checklist	4
Step 1: Installing PreAlert/TSO.....	8
1.1 Unloading Installation JCL	8
1.2 Unloading Installation Tape	9
1.3 Applying PreAlert Product Authorization and Maintenance	9
1.4 Specifying Userdata Options.	10
1.5 Authorizing PreAlert.	12
1.6 Initializing Statistics Logging	14
1.7 Starting PreAlert	16
1.8 Logging on to PreAlert/TSO	17
1.9 Using the PreAlert/TSO ISPF Interface	19
Step 2: Installing PreAlert/VTAM	21
2.1 Verifying PreAlert/TSO Installation	21
2.2 Defining the VTAM Application ID	21
2.3 Authorizing PreAlert.	22
2.4 Assessing Link Library Authorizations	22
2.5 Setting Security	22
2.6 Specifying Userdata Options.	22
2.7 Starting PreAlert	23
2.8 Log on to PreAlert/VTAM	24
2.9 Utilizing Extended Features	26
Step 3: Installing PreAlert/Local TSO	31
3.1 Adding TSO Authorized Program List	31
3.2 Using PreAlert/Local TSO	31

Overview

This chapter guides you through the PreAlert installation process. Once you have read this chapter, you are ready to proceed with the actual installation.

PreAlert can be installed under one or more of these environments: TSO/ISPF, VTAM, or native (local) TSO. This chapter provides an installation checklist and also explains each of these installations separately.

If you are installing PreAlert in more than one environment, ASG recommends that you perform the installation separately for each environment. However, you may install PreAlert simultaneously in more than one environment. This technique allows you to consolidate steps, such as updating and assembling the userdata macros for all environments at one time.

Installation questions that arise should be directed to the ASG Service Desk.

Installation Checklist

This section provides a checklist for you to follow as you install PreAlert. This is only a checklist. Full instructions explaining how to install PreAlert begin with ["Step 1 - Installing PreAlert/TSO" on page 8](#) and end with ["Step 3 - Installing PreAlert/Local TSO" on page 31](#).

The table below lists each installation milestone. Record the date each milestone is accomplished in the space provided.

Milestone	Date Accomplished
Step 1: Install PreAlert/TSO	_____
Step 1.1: Unload Installation JCL	_____
Step 1.2: Unload Installation Tape	_____
Edit UNLOAD Job	_____
Customize Jobcard	_____
Modify PREFIX Symbol for High-level Qualifier	_____
Modify DISKVOL Symbol for VOLSER	_____
Modify DISKUNT Symbol for Dataset UNIT Name	_____
Execute UNLOAD Job	_____

Milestone	Date Accomplished
Step 1.3: Apply Product Authorization and Maintenance	
Register and Activate This Release	
Review the PreAlert Maintenance Bulletin	
Step 1.4: Specify Userdata Options	
Edit USERDATA Member	
Choose UDPARMS Macro Keywords	
Specify UDAUSER Macros	
Specify IDMS Central Version (CV) Number and Jobname (IDMS only)	
Execute ASMUSRD Job or ASMHUSRD Job	
Step 1.5: Authorize PreAlert	
Edit TEMPAPF Job	
Customize the Jobcard	
Modify the Prefix Default	
Modify the APFLIB Default	
Execute TEMPAPF	
Step 1.6: Initialize Statistics Logging	
Edit the MLOGINIT Member	
Customize the Jobcard	
Modify the Prefix Default	
Specify BLKS, Log Data Size	
Specify OFFBLKS, Offload Data Size	
Execute MLOGINIT	
Edit the MLOGOFFL Member	
Customize the Jobcard	
Modify the Prefix Default	
Copy MLOGOFFL to the PreAlert Helpfile	
Edit the MLOGPRT1 and MLOGPRT2 Member	
Customize the Jobcard	

Milestone	Date Accomplished
Modify the Prefix Default	
Specify BLKS Default, Offload Data Size	
Step 1.7: Start PreAlert	
Edit the PAPROC Member	
Modify the Prefix Default	
Specify PARM=' VAP=*, SCR=MAINMENU'	
Copy PAPROC to a PROCLIB and Rename to PREALERT	
Start PreAlert	
Step 1.8: Log on to PreAlert/TSO	
Edit CLIST Member	
Modify Prefix Default	
Specify PARM (PAS=MTSO, SCR=MAINMENU) on PROC	
Copy to a TSO CLIST Library and Rename to PREALERT	
Execute PreAlert	
Step 1.9: Use the PreAlert/TSO ISPF Interface	
Execute PreAlert	
Add PreAlert to the ISPF Menu Panel (optional)	
Copy to PreAlert/TSO ISPF CLIST (optional)	
Step 2: Installing PreAlert/VTAM	
Step 2.1: Verify TSO Installation	
Step 2.2: Define VTAM Application ID	
Define the PreAlert NODE and APPL to VTAM	
Step 2.3: Authorize PreAlert	
Add Dataset Name and VOLSER	
Step 2.4: Assess Link Library Authorizations	
Step 2.5: Set Security	
Step 2.6: Specify Userdata Options	

Milestone	Date Accomplished
Edit the USERDATA Member	_____
Choose UDPARMS Macro Keywords	_____
Execute the ASMUSRD Job	_____
Step 2.7: Start PreAlert	_____
Edit the PAPROC Member	_____
Modify the Prefix Default	_____
Specify PARM=' SCR=MAINMENU '	_____
Copy PAPROC to a PROCLIB and Rename to PREALERT	_____
Start PreAlert	_____
Step 2.8: Log on to PreAlert/VTAM	_____
Step 2.9: Utilize Extended Features	_____
Step 3: Install PreAlert/Local TSO	_____
Step 3.1: Authorize the TSO Program List	_____
Add SHOPMON to the AUTHPGM and AUTHTSF lists	_____
Step 3.2: Use PreAlert/Local TSO	_____
Select CLIST1 or CLIST2 and Edit	_____
Dataset Prefix	_____
Modify PRTCLASS Default for SNAPFILE	_____
Modify the &DSNAME (CLIST2 Only)	_____
Add ALLOC and FREE for Exception Analysis Level Sets (optional)	_____
Copy CLIST into TSO CLIST Library and Rename to PATSO	_____
Execute the CLIST	_____

Step 1 - Installing PreAlert/TSO

Step 1 leads you through unloading the installation JCL and tape, applying product authorization and maintenance, specifying userdata options, authorizing PreAlert, initializing statistics logging, starting PreAlert, and using the PreAlert TSO/ISPF Interface.

The PreAlert/TSO installation procedure is designed for sites where an IPL is not possible in a timely fashion. This procedure provides the full features of PreAlert via TSO, including all authorized functions. The VTAM and local TSO user interfaces are not included as part of this procedure.

APF authorization is temporarily established by dynamically modifying the APF-authorized libraries list (IEAAPFxx) to include PreAlert. Since the list is modified in memory only, PreAlert will be authorized only for the life of the IPL. Should an IPL occur, execute the TEMPAPF job to reestablish APF authorization for PreAlert. For information on executing the TEMPAPF job, see ["1.5 Authorizing PreAlert" on page 12](#).

1.1 Unloading Installation JCL

This step unloads JCL at installation.

The first file of the PreAlert tape contains the JCL needed to unload the other datasets to disk. [Figure 2](#) shows a sample jobstream that may be used to unload the first file to a dataset.

Figure 2 • Sample JCL

```
//UNLOAD      JOB      . . . . .
//GO          EXEC    PGM=IEBGENER
//SYSPRINT    DD      SYSOUT=*
//SYSIN       DD      DUMMY
//SYSUT1      DD      DSN=PREALERT.INSTALL,DISP=(OLD,KEEP,KEEP),
//              UNIT=TAPE,VOL=SER=xxxx
//SYSUT2      DD      DSN=YOUR.FILE.NAME,
//              DISP=(NEW,CATLG,DELETE),
//              UNIT=SYSDA,SPACE=(3120,(50,10),RLSE)
//
```

Note that in VOL=SER=xxxx, xxxx is the value contained in the customer cover letter received with the product.

1.2 Unloading Installation Tape

The jobstream that was unloaded in the first step should now be customized to match your installation standards. Although this job should not require much modification, these items require your attention:

- Customize the jobcard.
- Modify the prefix symbol to a suitable high-level qualifier for the datasets (default is ASG.PREALERT).
- Modify the DISKVOL symbol to the VOLSER that the datasets are to be allocated on.
- Modify the DISKUNT symbol to the unit name that the datasets are to be allocated on.

After you have customized the unload job, execute it. This builds the files needed to complete the installation of PreAlert.

1.3 Applying PreAlert Product Authorization and Maintenance

In this section you will:

- Register and activate this release by applying the product authorization information.
- Review any PTFs that may relate to your environment and operating system and apply as required.

With the PreAlert product, the customer receives a product authorization document explaining how to register and activate the PreAlert product.

Run member ZAPJCL with the supplied values to authorize the product. [Figure 3](#) shows sample JCL added to run the ZAP of the authorization code to the product.

Figure 3 • Sample JCL

```
//USERID    JOB (ACCT), 'PAI AUTH', CLASS=A, MSGCLASS=X, NOTIFY=USERID
//*
//*
//*      DON'T FORGET TO CHANGE THE FOLLOWING SYMBOLICS -
//*
//*      PREFIX = HIGH LEVEL QUALIFIER FOR PREALERT LIBRARIES
//*
//*PRODAUTH  PROC    PREFIX='ASG.PREALERT'
//*
//*      APPLY PREALERT PRODUCT AUTHORIZATION ZAP
//*
//*ZAP1      EXEC PGM=IMASPZAP, PARM=IGNIDRFULL
//SYSPRINT  DD SYSOUT=*
//SYSUT1    DD DSN=&&SYSUT1, UNIT=SYSDA, SPACE=(CYL, (1,1))
//SYSLIB    DD DSN=&PREFIX..LINKLIB, DISP=SHR
```

```
/*  
//      PEND  
/*  
/*  
//PRODOOAUTH EXEC PRODAUTH  
//ZAP1.SYSIN DD      *  
      NAME SHOPMOND SHOPMKEY  
      REP 0000 xxxx, xxxx, xxxx, xxxx, xxxx, xxxx  
/*
```

Note:

In the example above the supplied authorization is entered in the field `xxxx`,
`xxxx, xxxx, xxxx, xxxx, xxxx`.

PreAlert generates the message PAV025 - PRODUCT AUTHORIZATION CODE INVALID if the PreAlert authorization is not applied or if it is applied incorrectly.

Review any PTFs that may relate to your environment and operating system. Apply the PTFs as required.

1.4 Specifying Userdata Options

The USERDATA member in the PreAlert control file (`xxxx.PREALERT.CNTL`) requires minimal tailoring to match your installation's needs. The following text lists the macros and keywords contained in the USERDATA member that are relevant to the installation process. For most installations, modifications to these options should suffice.

For a complete list of userdata macros and keywords, see ["Userdata Macros" on page 41](#).

In this step you will:

- Edit the USERDATA member.
- Choose UDPARMS macro keywords.
- Specify a list of authorized user ID(s) using the UDAUSER macro.
- For IDMS sites, specify the IDMS Central Version (CV) number and jobname for all IDMS CVs (UDCVNUM macro).
- Execute the ASMUSRD Job or ASMHUSRD Job.

UDPARMS Macro Keywords

Macro Keyword	Description
PIDMS=PRODIDMS	<p>For IDMS sites. Specifies the jobname of the production IDMS CV. This name will replace the PRODIDMS jobname found in the PreAlert pre-defined menus and tutorial screens.</p> <p>Note: _____ PRODIDMS provides only a default jobname. Any IDMS-CV may be monitored during PreAlert execution.</p>
TIDMS=TESTIDMS	<p>For IDMS sites. Specifies the jobname of the test IDMS CV. This name will replace the TESTIDMS jobname found in the PreAlert pre-defined menus and tutorial screens.</p> <p>Note: _____ TESTIDMS provides only a default jobname. Any IDMS-CV may be monitored during PreAlert execution.</p>
RMF=Y/N	<p>RMF is used to collect DASD, TAPE, and PAGE/SWAP dataset statistics.</p>
MTSOID=MTSO	<p>Specifies the PreAlert/TSO Interface ID as MTSO.</p> <p>Note: _____ Ensure an Interface ID value is specified.</p>
HELPDSN= *.PREALERT.HELP	<p>Specifies the dataset name allocated for each user's screen definitions. An asterisk (*) in any position is replaced with the user ID.</p>
UNIT=SYSDA	<p>Specifies the default DASD unit to use for dynamic allocation.</p>
MLOGDSN= *.PREALERT.MLOG	<p>Specifies the Statistics Logging dataset allocated for each PreAlert user. An asterisk (*) in any position is replaced with the user ID.</p>
SPFLPA=Y/N	<p>Specifies the location of ISPF. Specify Y if ISPF resides in the Link Pack Area (LPA) or N if it is not in the LPA.</p>
CHECK=YES	<p>Validates UDPARMS macro keywords.</p>

UDAUSER Macro Keywords

Specifies the list of authorized user IDs that are allowed access to PreAlert's restricted functions. The macro must be coded once for each authorized user ID. See ["UDAUSER Macro Options" on page 61](#) for a complete description.

UDCVNUM Macro Keywords

For IDMS sites, specify the CV number and the corresponding jobname for all IDMS CV's that may be monitored. This allows the user to use the IDMS CV number rather than the jobname with the IDMS line command. See ["UDCVNUM Macro" on page 66](#) for a complete description.

ASMUSRD Member

Customize the jobcard and the prefix default in the ASMUSRD member. After you have completed customizing the USERDATA member, execute the jobstream in this member.

1.5 Authorizing PreAlert

In this step you will:

- Edit the TEMPAPF job.
- Customize the jobcard.
- Modify the Prefix default to match the one used in ["1.2 Unloading Installation Tape" on page 9](#).
- Modify the APFLIB default to reflect the dataset name of an APF authorized library.

APF authorization is installed automatically by executing the TEMPAPF job in the PreAlert control file (xxxx.PREALERT.CNTL). This job links the SHOPMAPF program into an APF-authorized library and then executes it. The SHOPMAPF program dynamically adds the PreAlert link library (specified on the SHOPMLIB DD statement) to the APF-authorized library list.

The APF authorization of the PreAlert link library made by TEMPAPF exists only in memory; no permanent change is made to the MVS system datasets. Therefore, this change is in effect only for the life of the IPL and is destroyed at the next system IPL. Should an IPL occur, execute the TEMPAPF job again to restore PreAlert authorization.

Note:

For permanent APF authorization add the PreAlert link library to the IEAAPFxx PARMLIB member and IPL.

The TEMPAPF job requires only minimal tailoring:

- Modify the jobcard to match your installation standards.
- Change the prefix default to match the prefix used when the installation tape was unloaded.
- Change the APFLIB default to the dataset name of an APF-authorized library. Contact your systems programmer if you need the name of an authorized library or access to it.

After you have completed customizing the job, execute it. On successful completion, TEMPAPF will return a condition code of 0.

If TEMPAPF was unsuccessful, one of these user ABEND codes is returned:

ABEND Code	Description
100	TEMPAPF is not APF-authorized. The dataset specified for APFLIB is not included in the APF-authorized library list. Specify the dataset name of an existing APF-authorized library and rerun the job.
101	The SHOPMLIB DD statement was not found. Add the SHOPMLIB DD statement with DSN=xxxx.PREALERT.LINKLIB and rerun the job.
102	SQA storage GETMAIN failed. Sufficient SQA storage is not available to modify the APF-authorized library list. The PreAlert library cannot be authorized using TEMPAPF. See "1.5 Authorizing PreAlert" on page 12 for instructions on permanently authorizing PreAlert.
103	APF list full. The static APF list limit of 255 datasets has been reached. The PreAlert library cannot be authorized using TEMPAPF. See "1.5 Authorizing PreAlert" on page 12 for instructions on permanently authorizing PreAlert.
104	<p>CSVAPF add request failed. TEMPAPF received an error return code from the CSVAPF macro. TEMPAPF generates this message:</p> <pre>SHOPMAPF CSVAPF FAILED, return-code/reason-code</pre> <p>Return codes and reason codes are documented in <i>MVS/ESA SP V5 Auth Assembler Services References ALE-DYN</i>, GS28-1475.</p> <p>For return-code 0008 and reason-code 0804, the most common cause is that the user does not have RACF authorization to use CSVAPF. Refer to CSVAPF macro, environment for the RACF requirements for using the CSVAPF ADD feature, in the <i>MVS/ESA Auth Assembler Services</i> publication.</p> <p>For other codes contact the ASG Service Desk or see "1.5 Authorizing PreAlert" on page 12 for instructions on permanently authorizing PreAlert.</p>

A list of the runtime messages produced by PreAlert when authorization has been denied can be found under ["PreAlert Messages and Codes" on page 33](#).

1.6 Initializing Statistics Logging

In this step you will:

- Edit the MLOGINIT member.
- Customize the jobcard.
- Modify the prefix default.
- Specify BLKS, log data size.
- Specify OFFBLKS, offload dataset size.
- Execute MLOGINIT.
- Edit the MLOGOFFL member:
 - Customize the jobcard.
 - Modify the prefix default.
- Copy MLOGOFFL to the PreAlert Help file and rename to #MLOGOFF.
- Edit the MLOGPRT1 member:
 - Customize the jobcard.
 - Modify the prefix default.
 - Specify BLKS default, offload dataset size.

The PreAlert Statistics Logging feature records statistics and/or screen images to a set of log files. PreAlert records statistics to these datasets as requested by the user. When a dataset is filled, PreAlert will automatically submit a job to offload any full datasets. After the dataset has been offloaded, PreAlert may reuse it as the other datasets fill. The offloaded statistics are added to an offload dataset. The statistics are kept until printed and then deleted by the log print job.

The MLOGINIT member in the PreAlert control file contains the JCL needed to initialize two datasets to be used for statistics logging and to initialize the dataset to contain the offloaded data.

The JCL requires some tailoring:

- Customize the jobcard.
- Modify the prefix default to match the prefix used when the installation tape was unloaded.
- The size of the log dataset defaults to 1000 blocks (4096 bytes each). If you discover that the offload job is being run too often, increase the sizes of the datasets. The number of blocks is specified in the BLKS symbol on the PROC statement and the BLKS control record following the SYSIN DD.
- The size of the offload dataset defaults to 10,000 blocks. Adjust the OFFBLKS default to allow for the frequency of the MLOGPRT1 job.

After you have completed customizing the initialize job, execute it.

The Statistics Offload and Statistics Print jobs described below provide the means to offload and print the logged statistics. They do not provide a means for archiving the statistics; this is left to the user.

Statistics Offload

The MLOGOFFL member contains the JCL necessary to offload the statistics logging datasets. The statistics are offloaded to the OFFLOAD DD with a disposition of MOD. The JCL requires some tailoring:

- Customize the jobcard.
- Modify the prefix default to match the prefix used when the installation tape was unloaded.
- Copy the member to the PreAlert Help file and rename the member to #MLOGOFF. PreAlert will submit the job whenever a log dataset fills.

Statistics Print

The MLOGPRT1 member contains the JCL to print the offloaded statistics. The job should be run at least weekly to reallocate the offload dataset. The JCL requires some tailoring:

- Customize the jobcard.
- Modify the prefix default to match the prefix used when the installation tape was unloaded.
- The offload dataset is deleted and reallocated. The size of the dataset defaults to 10,000 blocks (4096 bytes each). Modify the BLKS default to allow for the frequency of the job.

The user may modify the JCL to archive the offloaded statistics.

The MLOGPRT2 member allows the user to extract and print statistics archived by the user. This JCL should be tailored similarly to the MLOGPRT1 JCL.

1.7 Starting PreAlert

A procedure to start PreAlert is included in member PAPROC of the PreAlert control file. This procedure requires some tailoring to match your installation's needs.

- Modify the dataset name prefix default to match the prefix used in unloading the installation tape.
- On the EXEC statement, specify `PARM='VAP=*,SCR=MAINMENU'`. This tells PreAlert to suppress the VTAM interface and to use the MAINMENU screen for the initial display. No other PARM keywords are needed.
- Copy the PAPROC member to a system procedure library (e.g., SYS1.PROCLIB), and rename the member to PREALERT.

After you have completed customization of the procedure, you may start PreAlert by entering `S PREALERT` on an MVS console. When PreAlert has completed its initialization, the message `PAV005 PREALERT/MTSO READY FOR LOGON` will be written to the MVS console.

Stopping PreAlert

The MVS stop command `P PREALERT` terminates PreAlert. The stop command allows for an orderly shutdown of any active user sessions and frees any CSA storage acquired by PreAlert. If PreAlert is cancelled, any acquired CSA storage will not be freed, possibly causing a CSA shortage.

Security Considerations

When a user logs onto PreAlert, PreAlert attempts to allocate a PDS for that user's screen definitions (see ["UDPARMS Macro Keywords" on page 11](#)). Therefore, PreAlert must have read, write, and allocate access to those files.

For IDMS users, PreAlert may dynamically allocate the IDMS log and journal files. PreAlert should have read access to the log and journal files for any IDMS CV to be monitored. PreAlert generates an error message if it is unable to allocate the files.

1.8 Logging on to PreAlert/TSO

A CLIST to execute PreAlert/TSO has been included in the PreAlert control file member CLIST3. This CLIST allocates the HELPFIL for PreAlert screen definitions and the SNAPFILE for dumps if PreAlert should abend. You can then execute PreAlert/TSO.

The CLIST requires some tailoring:

- Change the dataset name prefix default to match the prefix used when unloading the installation tape.
- On the PROC statement, specify `PARM (' PAS=MTSO, SCR=MAINMENU ')`. This specifies the PreAlert/TSO Interface ID and tells PreAlert to use the MAINMENU screen for the initial display.
- Copy the CLIST3 member to a TSO CLIST library (allocated by the SYSPROC DD statement in your TSO startup procedure) and rename the member to PREALERT.

The CLIST may now be executed by entering `%PREALERT` under the TSO READY prompt. PreAlert/TSO will send information shown in [Figure 4](#) to the terminal:

Figure 4 • Logon to PreAlert/TSO

```
PreAlert/TSO SIGNON SCREEN

ENTER USERID:  userid
      PASSWORD:

      SCREEN:  MAINMENU
SYSID=xxxx  CPU=3090/012345  MVS=SP6.0.4  PREALERT=V4.R2.0
```

Enter your TSO password and press Enter. PreAlert displays the startup screen as specified.

Bypass Signon Screen

By default, PreAlert does not require that you enter a password on the signon screen. The password is used by the security features as described in ["Security Considerations" on page 69](#). If you determine that the password is not required, you may bypass the PreAlert/TSO signon screen. Add the BPS=Y keyword to the parms on the PROC statement in the PREALERT clist. The PROC statement should appear like this:

```
PROC 0 PRTCLASS(X) PREFIX(ASG.PREALERT) +  
      PARM('SCR=MAINMENU,PAS=MTSO,BPS=Y')
```

With the BPS=Y, PreAlert bypasses the signon screen and immediately displays the MAINMENU screen.

Timeout Options

A timeout option may be specified for PreAlert/TSO sessions. When a PreAlert/TSO session has been idle for a period of time exceeding the timeout interval, the session either cancels or switches to a background session.

When a user leaves a PreAlert session unattended, it should be considered a security exposure. This could lead to the abuse of PreAlert's many powerful features. The timeout option was designed to help minimize this security exposure. Once a PreAlert/TSO session has timed out, the user must execute the PreAlert Clist to regain access to PreAlert. With the security features available in PreAlert, access may be secured.

Three UDPARMS macro keywords are used to control the timeout option:

MTIME=*nn* specifies the timeout interval

MHOLD=Y/N specifies whether to hold the session as a background session or to cancel the session (MHOLD=N)

MAUTO=Y/N specifies whether to turn on the Auto-update option if the timed out session is held (MHOLD=Y required)

With these parameters, you have four ways you can handle timeouts:

MTIME=0 default, no timeout interval. The PreAlert/TSO sessions are not checked for timeouts.

MTIME=*nnn* and MHOLD=N timeout occurs after *nnn* seconds and the session is cancelled.

MTIME=*nnn* MHOLD=Y and MAUTO=N timeout occurs after *nnn* seconds and the session is held idle as a background session.

MTIME=*nnn* MHOLD=Y and MAUTO=Y timeout occurs after *nnn* seconds and the session is held as a background session in Auto-update mode with the Auto-update interval set to either the last interval used, or the default specified in UDPARMS.

1.9 Using the PreAlert/TSO ISPF Interface

In this step you will:

- Execute PreAlert by keying %PREALERT at ISPF option 6.
- Add PreAlert to the ISPF menu panel (Optional).
- PreAlert/TSO ISPF CLIST (Optional).

PreAlert may be executed as a full function ISPF application by executing the Clist %PREALERT through ISPF option 6. PreAlert invokes the ISPF Dialog Management Services for all screen input and output. This permits the PreAlert user to take advantage of the many benefits of ISPF (e.g., split screen, jump screen).

The first line of all PreAlert screens will be `SPF COMMAND ==>`, allowing for the input of ISPF commands (e.g., `SPLIT`, `END`, `=X`). You must enter ISPF commands on the first line; PreAlert commands are entered in the `COMMAND` field on the second line.

For example, [Figure 5](#) shows ISPF in split screen mode with PreAlert:

Figure 5 • ISPF in split screen mode with PreAlert

```

----- ISPF/PDF PRIMARY OPTION MENU -----
OPTION ==>

      0  ISPF PARMS   - Specify terminal and user parameters      USERID   - DEVBER
      1  BROWSE       - Display source data or output listings    TIME      - 12:37
      2  EDIT         - Create or change source data              TERMINAL  - 3278
      3  UTILITIES    - Perform utility functions                PFKEYS    - 24
      4  FOREGROUND   - Invoke language processors in foreground
      5  BATCH        - Submit job for language processing
      6  COMMAND      - Enter TSO command or CLIST, or REXX exec

      . . . . .

SPF COMMAND ==>                                SCROLL ==> PAGE
COMMAND:      MAINMENU    12:38:08.5  97.345  75.37% .TUT FOR TUTORIAL
              PreAlert Primary Menu
.
.
.
MENU MVSMENU   :PREALERT/MVS INTERFACE
.
MENU IDMSMENU  :PREALERT/IDMS INTERFACE
.
MENU PAMENU    :PREALERT FUNCTIONAL FACILITIES
.
MENU SCREENS   :DISPLAY SCREENS LIST

```

Switching to a Background Session

After you have established your session, you may convert your session to a background session simply by entering the `.BGnn` control command (i.e., `.BG` to enter background without Auto-update, or `.BG5` to enter background with a five-second Auto-update interval).

PreAlert releases your terminal back to ISPF, but your PreAlert session continues to execute in the PreAlert address space exactly as it would if the terminal were still being used.

You may re-establish your PreAlert/ISPF session simply by executing the PreAlert CLIST again.

PreAlert Color Support

The PreAlert Color Terminal Support feature is supported under VTAM and ISPF.

PreAlert Auto-update

The PreAlert Auto-update feature is supported under ISPF. When Auto-update is active, the terminal keyboard will be locked, preventing any other activities on the terminal. To stop the Auto-update, press either the PA1 key for local terminals or the ATTN key for remote terminals. PreAlert will wait for the Auto-update interval to complete, then refresh the display and unlock the keyboard.

Caution! Users working on 3270 emulators must determine the correct key to stop PreAlert's Automatic Update feature. End the PreAlert session if you do not know the correct key to stop PreAlert's Automatic Update feature. The MVS modify command (F PREALERT, STOP, *userid*) may be used to terminate PreAlert sessions.

PF Key Definitions

The PreAlert PF key definitions are not used since the ISPF Dialog Manager passes all PF key activity as commands to the application. The ISPF key commands may be used to define PF keys for PreAlert commands. By using the ISPF menu panels with the PASPF CLIST, ISPF will maintain a separate set of PF key definitions for PreAlert.

ISPF Menu Panels (Optional)

PreAlert may be executed as an option of ISPF. The `SPF@PRIM` member in the PreAlert control file contains a standard ISPF primary menu panel modified to execute PreAlert as option P. This panel also assigns an ISPF application ID to PreAlert, allowing ISPF to maintain a separate set of PF key definitions for PreAlert.

PreAlert/TSO ISPF CLIST (Optional)

An additional CLIST, CLIST4, has been included in the PreAlert control file. This CLIST uses the ISPEXEC command to execute the PREALERT CLIST and to assign an ISPF application ID, allowing ISPF to maintain a separate set of PF key definitions for PreAlert.

CLIST4 should be copied to your TSO CLIST library and renamed to PASPF. PreAlert may then be executed by entering %PASPF through option 6.

Step 2 - Installing PreAlert/VTAM

Step 2 leads you through the PreAlert VTAM installation, which allows you to verify step ["1.1 Unloading Installation JCL" on page 8](#) through step ["1.4 Specifying Userdata Options" on page 10](#); define the VTAM application ID; authorize PreAlert; IPL the system; install the optional security exit; specify userdata options; start PreAlert; perform a PreAlert VTAM logon; and use extended features.

This step extends PreAlert functionality by establishing the PreAlert/VTAM interface and permanently authorizing PreAlert. This step may require an IPL before these functions are available.

2.1 Verifying PreAlert/TSO Installation

Sections ["1.1 Unloading Installation JCL" on page 8](#) through ["1.4 Specifying Userdata Options" on page 10](#) explain how to unload the PreAlert installation tape. Specific userdata options must be installed before proceeding.

2.2 Defining the VTAM Application ID

PreAlert must be defined as an application to VTAM by creating a new member (NODE) in SYS1.VTAMLST using these statements:

```
VBUILD TYPE=APPL
PREALERT APPL AUTH=(ACQ,NOTSO),PRTCT=PREALERT
```

Contact your telecommunications system programmer to add and activate the PreAlert NODE.

Note: _____

The APPLID (specified on the APPL statement as PREALERT) must not be the same as the NODE name (the member name in SYS1.VTAMLST).

2.3 Authorizing PreAlert

Since many of PreAlert's functions require APF authorization for execution, the PreAlert link library needs to be included in the IEAAPF_{xx} member of SYS1.PARMLIB. Do not forget to include the prefix and VOLSER you have chosen for the dataset.

Although APF authorization may be temporarily granted by using alternate methods, updating IEAAPF_{xx} is strongly recommended. This update will permanently authorize the PreAlert link library.

2.4 Assessing Link Library Authorizations

Sometime before you start PreAlert, an IPL may be required. This may be performed in order for the PreAlert library to become APF-authorized and to activate the PreAlert NODE and application ID in VTAM.

2.5 Setting Security

PreAlert provides optional security features to allow the user to impose additional security measures above and beyond the concept of authorized users. The security features may be used to grant authorization to users and to restrict the use of the more sensitive functions to certain users. Review ["PreAlert Messages and Codes" on page 33](#) for complete instructions on coding and installation of the security exit.

2.6 Specifying Userdata Options

In addition to the items specified in ["1.4 Specifying Userdata Options" on page 10](#), other userdata items should be reviewed.

UDPARMS Macro Keywords

Macro Keywords	Description
AUTHXIT=Y/N	The user security exit is used to allow/deny authorization to user IDs not included in the UDAUSER macros.
SECINT=Y/N	Restricts the use of the Auto-update option to authorized users.
SECSAVE=Y/N	Restricts the use of the Screen Save option to authorized users.
SECWAIT=Y/N	Restricts the use of the PreAlert Wait Analysis function to authorized users.
VAPPL=PREALERT	Specifies the VTAM application ID for PreAlert.
VPASS=PREALERT	Specifies the VTAM application password for PreAlert from the (PRTCT=PREALERT PARM).

Macro Keywords	Description
VTAMMAX=4	Specifies the maximum number of concurrent PreAlert VTAM or TSO sessions.
VTIME=900	Specifies the user session timeout interval in seconds. See VHOLD also.
VHOLD=Y/N	Requests that the session be held (Y) or closed (N) when a user session times out.
VDATA=Y/N	Requests that PreAlert accept (Y) or ignore (N) logon data for the user ID and password.
VSWAP=Y/N	Requests that PreAlert be run swappable (Y) or non-swappable (N).

For most installations, the above-mentioned modifications should suffice. For a complete list of userdata macros and keywords, refer to ["Userdata Macros" on page 41](#). After you have completed customizing the USERDATA member, execute the jobstream in the ASMUSRD member.

2.7 Starting PreAlert

The PreAlert control file member PAPROC includes a procedure to start PreAlert. This procedure requires some tailoring to match your installation's needs.

- Modify the dataset name prefix default to match the prefix used when unloading the installation tape.
- On the EXEC statement, specify `PARM= ' SCR=MAINMENU '`. This tells PreAlert to use the MAINMENU screen for the initial display. No other PARM keywords should be used.
- Copy the PAPROC member to a system procedure library (e.g., SYS1.PROCLIB), and rename the member to PREALERT.

After you have completed customization of the procedure, you may start PreAlert by entering `S PREALERT` on an MVS console. When PreAlert has completed its initialization, the message `PAV005 - PREALERT/VTAM READY FOR LOGON` will be written to the MVS console. PreAlert will then accept either VTAM or TSO session logons.

Stopping PreAlert

The MVS stop command `P PREALERT` may be used to terminate PreAlert. The stop command provides an orderly shutdown of any active user sessions and frees any CSA storage acquired by PreAlert. If PreAlert is cancelled, any acquired CSA storage will not be freed, possibly causing a CSA shortage.

VTAM Multi-Session Software

Attempting to use PreAlert/VTAM through software that provides multiple session capabilities may cause unpredictable results. Often these programs intercept VTAM return and feedback codes needed by PreAlert for the Auto-update function.

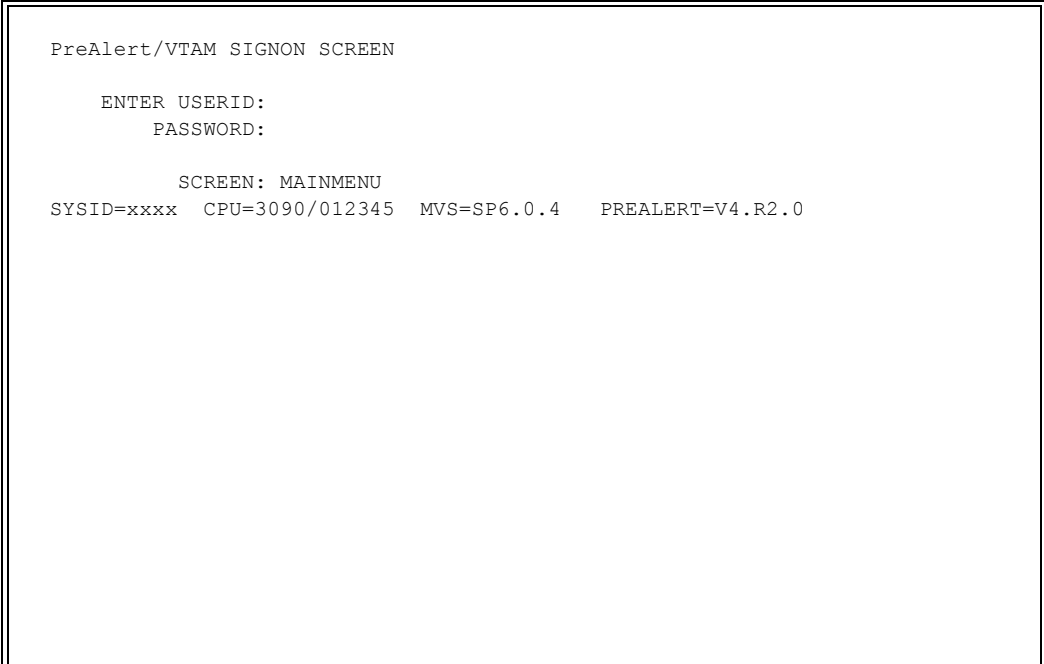
2.8 Log on to PreAlert/VTAM

To log on to a PreAlert/VTAM terminal session, enter one of these commands through your VTAM Logon screen:

```
LOGON APPLID(applid)  
LOGON APPLID(applid) DATA(TSO userid/password)  
LOGON APPLID(applid) DATA(TSO userid/password,screen)
```

If the first logon format was used, PreAlert sends the following information to the terminal (shown in [Figure 6](#)).

Figure 6 • PreAlert/VTAM SIGNON SCREEN



```
PreAlert/VTAM SIGNON SCREEN  
  
ENTER USERID:  
PASSWORD:  
  
SCREEN: MAINMENU  
SYSID=xxxx CPU=3090/012345 MVS=SP6.0.4 PREALERT=V4.R2.0
```

Enter your TSO user ID and password (non-display field) in the designated fields. PreAlert will display the startup screen as specified.

Security Considerations

When a user signs on, PreAlert attempts to allocate a PDS for that user's screen definitions. Therefore, PreAlert must have read, write, and allocate access to those files.

For IDMS users, PreAlert may dynamically allocate the IDMS log and journal files. PreAlert should have read access to the log and journal files for any IDMS CV to be monitored. PreAlert generates an error message if it is unable to allocate the files.

Switching to a Background Session

After you have established your session, you may convert your session to a background session by entering the `.BGnn` control command (i.e., `.BG` to enter background without Auto-update or `.BG5` to enter background with a five-second Auto-update interval).

PreAlert will release your terminal back to VTAM, but your PreAlert session will continue to execute in the PreAlert address space exactly as it would if the terminal was still being used. You may re-establish your PreAlert session by following the VTAM logon procedure or the TSO logon procedure.

Timeout Options

A timeout option may be specified for PreAlert/VTAM sessions. When a PreAlert/VTAM session has been idle for a period of time exceeding the timeout interval, the session either cancels or switches to a background session.

When a user leaves a PreAlert session unattended, it should be considered a security exposure. This could lead to the abuse of PreAlert's many powerful features. The timeout option was designed to help minimize this security exposure. Once a PreAlert/VTAM session has timed out, the user must logon to PreAlert to regain access to PreAlert. With the security features available in PreAlert, access may be secured.

Three UDPARMS macro keywords are used to control the timeout option:

`VTIME=nn` specifies the timeout interval

`VHOLD=Y/N` specifies whether to hold the session as a background session, or to cancel the session (`VHOLD=N`)

`VAUTO=Y/N` specifies whether to turn on the Auto-update option if the timed out session is held (`VHOLD=Y` required)

With these parameters, you have four ways to handle timeouts:

`VTIME=0` default, no timeout interval. The PreAlert/VTAM sessions are not checked for timeouts.

`VTIME=nnn` and `VHOLD=N` timeout occurs after `nnn` seconds, the session is cancelled.

`VTIME=nnn`, `VHOLD=Y`, and `VAUTO=N` timeout occurs after `nnn` seconds, the session is held as an idle background session.

VTIME=*nnn*, VHOLD=Y, and VAUTO=Y timeout occurs after *nnn* seconds, the session is held as a background session in Auto-update mode with the Auto-update interval set to either the last interval used, or the default specified in UDPARMS.

2.9 Utilizing Extended Features

The following text details PreAlert's extended features.

Auto-start Sessions

A session may automatically start when PreAlert is started. This allows the user to have a PreAlert session begin monitoring immediately and eliminates any need for manual intervention just to start a session.

To automatically start a session, specify a user ID or a password. The user ID and password may be specified through either a sequential dataset, or as keywords in the PreAlert startup JCL. However, only the user ID and password may be specified in the file; any other parameters must be entered using the keywords in the PreAlert startup JCL.

Use the AUSRPASS DD statement is used to specify the sequential dataset that contains the user ID and password for the Auto-start session. The DD statement is formatted like this:

```
//AUSRPASS DD DSN=auto.start.file,DISP=SHR
```

The AUSRPASS dataset should contain a single record specifying the user ID and optional password. The user ID must begin in column 1 and is followed by a slash (/) and the password. The format of the record looks like this:

```
USERID/PASSWORD
```

Limit the user ID and password to no more than eight characters each.

These keywords are used in the PreAlert startup JCL:

Keywords	Description
USR= <i>user ID</i>	User ID for the Auto-start session.
UPW= <i>password</i>	Password for the user ID.
USC= <i>screen name</i>	Startup screen name for the Auto-start session. If this keyword is not specified or found, defaults to the screen name from the SCR= keyword.
URL= <i>nnn</i>	Auto-start session restart limit. If the Auto-start session abends, PreAlert will automatically restart the session. The URL keyword limits the number of times the session will be restarted.

Keywords	Description
	URL=0 will suppress the restart.
	URL=5 will allow five restarts.
	URL=* will allow restarts indefinitely.
	The default is 0 (no restarts).
VTM= <i>LU-name</i>	LU-name of the VTAM terminal for the Auto-start session. PreAlert will acquire the terminal at startup. If VTM= is not specified, the Auto-start session will be started as a background session.
VLM= <i>logmode</i>	Name of a VTAM log mode entry used to override the default log mode entry associated with the Auto-start terminal.

The minimum required keywords for Auto-start sessions are as follows:

- Background session:
`USR=user ID`
`UPW=password`
- VTAM terminal session:
`USR=user ID`
`UPW=password`
`VTM=LU-name`

Started Sessions

After starting PreAlert, you can start additional sessions using the MVS Modify command. This feature allows you to start additional PreAlert sessions to monitor specific IDMS regions. As an IDMS region is started, an MVS Modify command is issued for PreAlert to start a session just to monitor the IDMS region. As other IDMS regions are started, more Modify commands are used to start more PreAlert sessions to monitor those IDMS regions.

The format of the MVS Modify command is described in ["PreAlert Operator Commands" on page 28](#).

Each started session requires a unique user ID. An optional password may also be used. If the password was not specified in the Modify command, then PreAlert reads the SUSRPASS dataset to obtain a password for the user ID. If the user ID is not located in SUSRPASS, then the session is started without a password.

The SUSRPASS DD statement is used to specify the sequential dataset that contains the user IDs and passwords for started sessions. The DD statement is formatted like this:

```
//SUSRPASS DD DSN=started.sessions.file,DISP=SHR
```

The SUSRPASS file should contain a record for each started session user ID. The user ID must begin in column 1 and is followed by a slash (/) and the password. The format of the records looks like this:

```
USERID/PASSWORD
```

The user ID and password should be limited to no more than eight characters each.

PreAlert Operator Commands

The MVS STOP command P PREALERT terminates all user sessions and PreAlert/VTAM.

The MVS MODIFY command F PREALERT displays the active sessions; stops all active sessions and terminates PreAlert; stops a specified session; or starts a session:

```
F PREALERT,DISPLAY
```

```
F PREALERT,STOP
```

```
F PREALERT,STOP,userid
```

```
F PREALERT,START,userid/password,screen,url,lu-name,logmode
```

The modify command uses positional parameters. The parameters must be specified in the order shown.

Optional Command	Description
DISPLAY	Message PAV011 is issued indicating user ID and logical unit for all sessions.
STOP,userid	Cancels the session with the specified user ID.

Optional Command	Description
<code>START,userid/ password, screen,url, lu-name, logmode</code>	<p>Userid—user ID for the started session, required.</p> <p>Password—password for the user ID, optional.</p> <p>Screen—Initial screen name, optional. If not specified, PreAlert will use the screen name specified in the SCR=screen parameter in the PreAlert start up procedure.</p> <p>url—Session restart limit. If the started sessions abends PreAlert will automatically restart the session. The url value limits the number of times the session will be restarted.</p> <p>0 suppresses the restart option.</p> <p>5 allows five restarts.</p> <p>* allows restarts indefinitely.</p> <p>The default is zero, no restarts.</p>
<code>START,userid/ password, screen,url, lu-name, logmode</code>	<p>Lu-name—LU-name of the VTAM terminal for the started session. PreAlert will acquire the terminal. If lu-name is not specified, the started session will be started as a background session.</p> <p>Logmode—Name of a VTAM log mode entry used to override the default log mode entry associated with the started session terminal.</p> <p>These are the minimum required parameters for a started session:</p> <ul style="list-style-type: none"> Start a background session: F PREALERT, START, <i>userid</i> Start a background session using a specified screen: F PREALERT, START, <i>userid/password, screen</i> Start a VTAM terminal session using a specified screen: F PREALERT, START, <i>userid/password, screen, lu-name</i>

Multiple PreAlert Tasks

If you have chosen to have PreAlert automatically start a session, you may want to consider running separate PreAlert tasks: one for the Auto-start Session and another for normal PreAlert/VTAM and PreAlert/TSO users. This also should be done if you are in a multiple system environment (more than one physical CPU or LPAR).

- Add additional VTAM APPL statements as necessary for each PreAlert task.
- Create additional startup PROCS, including startup keywords.

Keywords	Description
PAS= <i>xxxx</i>	PreAlert/TSO Interface ID
VAP= <i>Applid</i>	VTAM application ID
VPS= <i>Password</i>	VTAM Application Password

- Create additional TSO CLISTs with the PAS=*xxxx* keyword specified to match the startup PROCS.

Note:

The PreAlert TSO interface will work only within a single system. The VTAM interface must be used to communicate across multiple systems.

ALTHELP File

The optional ALTHELP DD may be used to specify the name of a partitioned dataset that holds your installation tailored screens. The alternate help file provides a convenient means of saving installation tailored screens across different releases of PreAlert. When this file is used, PreAlert will search it before searching the system help file.

This is the format of a DD statement:

```
//ALTHELP DD DSN=&PREFIX..ALTHELP,DISP=SHR
```

The ALTHELP file should be allocated using the same logical record length and blocksize as the PreAlert system helpfile.

SHOPMLIB File

An additional DD statement may be added to the startup JCL to allow MVS and/or IDMS Exception Analysis level sets to be loaded from non-APF-authorized libraries. As a result, the installation can write-protect the PreAlert LINKLIB (which is APF-authorized) while users can still assemble their own Exception Analysis level sets.

This is the format of the DD statement:

```
//SHOPMLIB DD DSN=user.exception.levels,DISP=SHR
//           DSN=&PREFIX..SHOPMON.LINKLIB,DISP=SHR
```

By allocating SHOPMLIB to the *user.exception.levels* library and concatenating the PreAlert LINKLIB to it, the user can load Exception Analysis level sets from either dataset.

ASG-IMPACT and ASG-Server Facility

PreAlert can automatically route MVS or IDMS exception messages to the ASG-Server Facility. The Event Notification Manager within the server passes the exception message to some other software, such as ASG-IMPACT, which is responsible for transforming the exception into a problem management entity.

An additional DD statement is added to the PreAlert startup JCL to identify the load library for the ASG-Server Facility.

This is the format of the DD statement:

```
//ASFLINK DD DSN=asf.v110.loadlib,DISP=SHR
```

Refer to the chapter on Exception Analysis in the *ASG-PreAlert IDMS User's Guide* for details on routing messages to the service facility and the format of the data being sent.

Step 3 - Installing PreAlert/Local TSO

Step 3 leads you through setting up TSO Authorized Program List and using PreAlert with local TSO.

PreAlert/Local TSO may not be executed under ISPF. PreAlert requires APF authorization, but ISPF runs non-authorized, thus anything running under ISPF loses APF authorization. The PreAlert/Local TSO Clists use the TSOEXEC command to execute PreAlert separate from ISPF.

3.1 Adding TSO Authorized Program List

Add SHOPMON to the AUTHTSF and AUTHPGM lists in the IKJTSO_{xx} member in SYS1.PARMLIB. Issue the PARMLIB UPDATE(_{xx}) command after IPL to dynamically change the IKJTSO_{xx} member. The TSO/E PARMLIB UPDATE command replaces the current IKJTSO_{xx} with the member specified in the command.

3.2 Using PreAlert/Local TSO

Two Clists have been included in the PreAlert control file, CLIST1 and CLIST2. In CLIST1, any screens saved by the user are written to the PreAlert help file (HELPPFILE). In CLIST2, the screens are written to the user's own help file (SCRNFILE). Note, in CLIST2, PreAlert dynamically allocates the user's own help file if one has not been found.

In the desired member (CLIST1 or CLIST2), these items may require your attention:

- Change the dataset name prefix default to match the prefix used when unloading the installation tape.
- Change the default SYSOUT class (PRTCLASS) for the SNAPFILE (used to print snap dumps if PreAlert shouldabend).
- In CLIST2 only, change the dataset name in the SET &DSNAME statement to match the HELPDSN= keyword when specifying the userdata options. Also, replace the asterisk (*) with &SYSUID.
- The SHOPMLIB file for Exception Analysis level sets may be allocated by adding this ALLOC command:

```
ALLOC FI (SHOPMLIB) DA ('user.exception.levels', +  
                        '&PREFIX..LINKLIB') SHR
```

Also, a FREE command should be added after the CALL to PreAlert:

```
FREE FI (SHOPMLIB)
```

- Copy the member into a TSO CLIST library (allocated by the SYSPROC DD card in the TSO startup PROC) and rename it to PATSO.

Enter %PATSO under the TSO READY prompt to execute the CLIST .

3

PreAlert Messages and Codes

The PreAlert Messages and Codes chapter contains these sections:

PreAlert Started Task Messages	33
PreAlert Abend Codes	38
PreAlert Abend Summary	38
PreAlert User Abend Codes	39
Authorization Messages	40

PreAlert Started Task Messages

PAV000 - Text

A problem was encountered while attempting to initiate a background session.
Text contains the message text normally displayed on the PreAlert Signon screen.

PAV001 - HELPFILE NOT ALLOCATED

The HELPFILE (PreAlert screen definitions) DD statement was not found. PreAlert terminates with a return code of 8.

PAV002 - MLOGFILE DCB ATTR INVALID, DD IGNORED

The DCB attributes for the MLOGFILE DD statement are invalid. The DD statement is ignored. User session should allocate their own files through the MLOG line command. Refer to "Statistics Logging Feature" in the *ASG-PreAlert IDMS User's Guide* or the *ASG-PreAlert MVS User's Guide* for the correct DCB attributes.

PAV003 - VTAM OPEN ACB FAILED, ERROR=xx

An error occurred while opening the VTAM ACB. xx contains the ACB error flag (hexadecimal). Refer to IBM's VTAM Programming publication for a complete list of ACB errors. PreAlert/VTAM terminates with a return code of 8.

x'24'- The ACB password does not match the password specified in the corresponding APPL.

x'56'- The user supplied APPLID was found, but it was for an entry other than an APPL entry.

x'58'- Another program has already opened the APPL.

x'5A'- The user supplied APPLID was not found in VTAM.

PAV004 - VTAM [SIMLOGON |SETLOGON] FAILED,
RPL-RTNCD/FDBK2=xx/xx, SENSE=xxxx

SIMLOGON - An error occurred when the SIMLOGON macro was issued to Auto-start a terminal session.

SETLOGON - An error occurred when the SETLOGON macro was issued to allow session logons.

The RPL return code, feedback code, and sense data is shown. Refer to the IBM VTAM Programming publication for a description of the codes. PreAlert/VTAM terminates with a return code of 8.

PAV005 - PREALERT[VTAM |MTSO] READY FOR LOGON

PreAlert has completed initiation and is ready to accept logon(s) from VTAM terminals or TSO sessions.

PAV006 - LOGON FAILED, INSUFFICIENT REGION

During logon processing for a user session, a GETMAIN failed, indicating insufficient region. The user session is terminated, but PreAlert continues executing.

PAV007 - OPNDST FAILED, RPL-RTNCD/FDBK2=xx/xx, SENSE=xxxx

During logon processing for a user session, an error occurred when the OPNDST macro was issued for the terminal. The RPL return code, feedback code, and sense data are shown. The user session is terminated, but PreAlert continues execution.

PAV008 - TPEND EXIT ENTERED, SESSIONS TERMINATED

The TPEND exit routine was entered in response to VTAM being shut down. All user sessions are terminated and PreAlert terminates.

PAV009 - LOST TERM EXIT ENTERED FOR LU:luname/userid SESSION TERMINATED

The Lost Term exit routine was entered for the logical unit and user. The user session is terminated with the return code set to the Lost Term reason code from VTAM.

PAV010 - userid/luname SESSION ABENDED [S |U]xxx

An abend occurred for the indicated user session. Refer to ["PreAlert Abend Codes" on page 38](#) for a list of PreAlert abend codes. Contact the ASG Service Desk for additional assistance.

PAV011 - userid/luname ACTIVE

This message is generated in response to an F PREALERT,DISPLAY operator command. The user has a session active on the logical unit shown.

PAV012 - VTAM [SEND |RECEIVE] FAILED LU:*userid/luname*
RTNCD/FDBK2=*xx/xx*, SENSE=*xxxx*

An error has occurred during a SEND or RECEIVE operation for the indicated user session. The return code, feedback code, and sense data are also shown. Refer to IBM's VTAM Programming publication for explanations of the codes. The user session is abended with a U2002 for SEND errors, and a U2003 for RECEIVE errors.

PAV013 - WARNING, PREALERT NOT APF AUTHORIZED

PreAlert has been executed from a non-APF-authorized library. None of the PreAlert authorized functions will be available.

PAV014 - PREALERT/*xxxx* ALREADY STARTED

A PreAlert session with the same PreAlert/TSO Interface ID is already being executed. The PreAlert/TSO Interface ID is specified in either the PAS=*xxxx* startup keyword or the MTSOID=*xxxx* USERDATA keyword.

PAV015 - TSO USER:*userid* NOT RESPONDING

A timeout occurred while PreAlert/TSO was waiting for a TPUT command to complete for the TSO user. The PreAlert/TSO session will be terminated.

PAV016 - MTSO LOGON FAILED FOR USER *userid*

The ASCB validation routines for Cross Memory Post failed during logon processing for a PreAlert/TSO session with the TSO user. The session is terminated.

PAV017 - ASCB VALIDATION FAILED FOR *userid* - SESSION TERMINATED

The ASCB validation routines for Cross Memory Post failed during a PreAlert/TSO session with the TSO user. The session is terminated.

PAV018 - MODIFY PREALERT COMMAND COMPLETE

PreAlert has completed processing of the Modify the F PREALERT command.

PAV019 - MLOGFILE DD NOT REQUIRED

PreAlert found a DD statement for the MLOGFILE when the multiple MLOG files (MLOG1, MLOG2, etc) were specified. The MLOGFILE DD statement is ignored.

PAV020 - INTRDR DD REQUIRED, PREALERT STOPPED

The INTRDR DD statement was not included in the PreAlert startup JCL. An INTRDR DD statement is required when the multiple MLOG files are used.

PAV021 - OFFLOAD JCL MEMBER *name* NOT FOUND

The indicated member name was not found in the PreAlert Help file. This member contains the JCL to offload the multiple MLOG datasets. The MLOGOFFL member of the PreAlert control file should be customized, copied to the Help file, and renamed to the *name* indicated in the message.

PAV022 - PREALERT LOG OFFLOAD JOB SUBMITTED

PreAlert has submitted the job to offload the multiple MLOG datasets. The job is submitted when PreAlert encounters a full MLOG dataset.

PAV023 - MODIFY COMMAND NOT RECOGNIZED

PreAlert did not recognize the verb specified in the modify the F PREALERT command. The modify command is ignored.

PAV024 - LOG DATA SET SWITCH COMPLETE

PreAlert has successfully switched recording to another log dataset in response to an F PREALERT, SWITCH command. The previous log (MLOG) dataset has been marked as CLOSED and the log offload job will also be submitted also.

PAV025 - PRODUCT AUTHORIZATION CODE INVALID

The PreAlert product authorization code is incorrect. The product authorization code is installed via a zap. ["1.5 Authorizing PreAlert" on page 12](#) of the PreAlert installation procedure tells how to install this zap. This message indicates that the check digit within the production authorization is incorrect, typically caused when the code is applied incorrectly.

PAV026 - PREALERT NOT LICENSED FOR CPU xxxxx

PreAlert has not been licensed to execute on the CPU. xxxxx indicates the CPU serial number. Contact the ASG Service Desk for an updated product authorization code.

PAV027 - PREALERT LICENSE HAS EXPIRED

The license for PreAlert has expired. Contact the ASG Service Desk for an updated product authorization code.

PAV028 - userid SESSION RESTART REQUESTED

The PreAlert Auto-start or started session has terminated. PreAlert is restarting the session. See ["Auto-start Sessions" on page 26](#) or ["Started Sessions" on page 27](#) for further information.

PAV029 - userid SESSION RESTART LIMIT REACHED

The PreAlert Auto-start or started session has been terminated. PreAlert will not restart the session because the restart limit has been reached. See ["Auto-start Sessions" on page 26](#) or ["Started Sessions" on page 27](#) for further information.

**PAV030 - VTAM [SEND|RECEIVE] FAILED LU:userid/luname
RTNCD/FDBK2=xx/xx, SENSE=xxx**

An error has occurred during a SEND or RECEIVE operation for the indicated user session. The return code, feedback code, and sense data are also shown. Refer to IBM's VTAM Programming publication for explanations of the codes. The user session terminates.

PAV031 - MTSO ID OR VTAM APPL REQUIRED, PREALERT STOPPED

Neither the MTSO ID or the VTAM APPLID has been specified. One or both of these must be specified in either the PreAlert userdata or in the startup procedure. In the userdata, use the MTSOID=*mtsoid* and VAPPL=*applid* keywords. In the startup procedure, use the PAS=*mtsoid* and VAP=*applid* keywords.

PAV032 - PREALERT USERDATA ASSEMBLED: MM/DD/YY HH:MM

PreAlert is using the userdata macro assembled on the indicated date at the indicated time. This message allows the user to verify that the appropriate userdata macro is being used by PreAlert.

PAV033 - ALTHELP DSORG MUST BE PO

The ALTHELP DD does not specify partitioned dataset. The dataset must be partitioned, DSORG=PO. PreAlert terminates with a return code of 8.

PAV034 - PREALERT WAITING ON *userid*

While processing a STOP command, PreAlert is waiting on terminal input from the indicated TSO user. If terminal input occurs within 25 seconds, PreAlert completes the STOP command normally. If no terminal input occurs within 25 seconds, PreAlert generates message PAV035 and continues processing the STOP command.

PAV035 - 256 BYTES CSA NOT FREED FOR *userid*

In response to a terminal input timeout described in message PAV034, PreAlert could not free the CSA communication area since it was still being accessed by the TSO user.

PAV036 - *userid* SESSION START REQUESTED

PreAlert has received a modify command to start a session. PreAlert is starting the session as requested.

PAV037 - INVALID START REQUESTED, USERID REQUIRED

PreAlert has received a modify command to start a session. The modify command did not contain a user ID. A user ID must be included with the modify start command.

PAV038 - INVALID START REQUEST, *userid* ACTIVE

PreAlert has received a modify command to start a session. The modify command specified a user ID for a session that is currently running. Each session must have a unique user ID.

PAV039 - PREALERT type USER *userid*/termid SIGNED ON

This message is generated when a user signs on to PreAlert. The type may be MTSO for a PreAlert TSO user session, AUSR for auto-start session, or VTAM for a PreAlert VTAM user session.

PAV040 - PREALERT type USER userid/termid RECONNECTED TO BACKGROUND SESSION

This message is generated when a user reconnects to a background session. The type may be MTSO for a PreAlert TSO user session, AUSR for auto-start session, or VTAM for a PreAlert VTAM user session.

PreAlert Abend Codes

Should an abend occur in PreAlert, PreAlert will produce a SNAP dump. For multiple user sessions, the dump will be in a SYSOUT file allocated to the PreAlert started task. For Local TSO sessions, the dump will be in a SYSOUT file (DDNAME = SNAPFILE) allocated to your TSO session.

Note:

Locate the SNAP dump prior to contacting ASG Service Desk.

PreAlert Abend Summary

If the PreAlert abend detection routines were able to determine that the error occurred within PreAlert, it will print an abend summary at the beginning of the SNAP dump, as shown in [Figure 7](#).

Figure 7 • Abend Summary

```

PREALERT ABEND SUMMARY
ABEND=00000000 PROGRAM=00000000 VERSION=V0.R0.0
OFFSET=00000000 PSW=00000000 00000000
R0-3  00000000 00000000 00000000 00000000
R4-7  00000000 00000000 00000000 00000000
R8-11 00000000 00000000 00000000 00000000
R12-15 00000000 00000000 00000000 00000000
  
```

The abend summary contains this information:

Field	Description
ABEND=00 <i>sssuuu</i>	<i>sss</i> is the System Abend code in HEX <i>uuu</i> is the User Abend code in HEX
PROGRAM= <i>pgm-name</i>	PreAlert program name
VERSION= <i>Vx.Rx.x</i>	PreAlert version.release
OFFSET= <i>xxxxxxxx</i>	Offset into the program where the abend occurred

Field	Description
PSW=xx.....xx	Program Status Word at the time of error
R0-3=xx.....xx	Registers 0 through 3 at the time of error
R4-7=xx.....xx	Registers 4 through 7
R8-11=xx.....xx	Registers 8 through 11
R12-15=xx.....xx	Registers 12 through 15

If the abend summary was not produced, please locate the RTM2WA SUMMARY in the SNAP dump, then contact ASG Service Desk.

PreAlert User Abend Codes

Abend Code Dec:Hex	Description
600:258	PreAlert has detected an internal loop through the STIMER TASK exit routine. Contact the ASG Service Desk.
601:259	Insufficient region for PreAlert to initialize. The region size should be increased.
602:25A	Insufficient region for PreAlert to format more than 127 logical display lines. Either increase the region size or reduce the number of display lines.
700:2BC	PreAlert received an invalid return code from an ISPF request. Contact the ASG Service Desk.
701:2BD	PreAlert HELPFILE not allocated. The CLIST being used must include this command: <code>ALLOC FI (HELPFIL) DA (your.PREALERT.HELPFIL) SHR</code> Where <i>your</i> is your site's PreAlert high-level qualifier.
702:2BE	PreAlert was unable to locate the JFCB for the HELPFIL. Contact the ASG Service Desk.
703:2BF	PreAlert received an invalid return code from an ISPF request. Contact the ASG Service Desk.
799:31F	PreAlert detected an abend in the ISPF interface subtask. Contact the ASG Service Desk.
2001:7D1	An internal error has occurred in PreAlert/VTAM. Contact the ASG Service Desk.

Abend Code Dec:Hex	Description
2002:7D2	A PreAlert/VTAM session has received a non-zero return code from the SEND/CHECK macros. Message PAV012 is issued showing the return code, feedback code, and sense data. Only the session is abended. PreAlert continues executing.
2003:7D3	A PreAlert/VTAM session has received a non-zero return code from the RECEIVE/CHECK macros. Message PAV012 is issued showing the return code, feedback code, and sense data. Only the session is abended. PreAlert continues executing.
2004:7D4	An internal error has occurred in PreAlert/VTAM. Contact the ASG Service Desk.
3333:D05	The PreAlert/TSO terminal input and output routines have detected input and output errors. Contact the ASG Service Desk.

Authorization Messages

When PreAlert has been denied APF authorization, the .ATH line command will display one of these messages:

PREALERT NOT AUTHORIZED

This message indicates that PreAlert is not APF-authorized. Possible causes depend on the method of authorization being used, as follows:

For PreAlert/Local TSO ISPF or PreAlert VTAM:

- The PreAlert LINKLIB is not in the APF list.
- PreAlert has been linked without AC=1.

USER NOT ALLOWED AUTH

Your TSO user ID was not included in the list of authorized user IDs in the PreAlert USERDATA member or was disallowed by the Security Exit.

4

Userdata Macros

This chapter discusses the userdata macros available with the PreAlert product. These sections are included in this chapter:

UDPARMS PreAlert User Installation Data	42
UDPARMS Macro Example for PreAlert/TSO Userdata Options	42
UDPARMS Macro Example for PreAlert/VTAM Userdata Options	43
UDPARMS Option Cross-reference	43
UDPARMS Option Descriptions	48
User Authorization and Security Options	48
Print Options	51
Message Options	51
Statistics Logging Options	51
Color/Highlighting Options	52
Miscellaneous Options (of General Scope)	53
IDMS Options	55
ASG-SIRF Options	58
MVS Options	58
VTAM Options	59
TSO Options	60
ASG-SERVER FACILITY Options	61
UDAUSER Authorized User IDs	61
UDLCX Line Command Exclude Feature	62
UDCHATT Special Character Attributes	63
UDPGN MVS Performance Group Names	63
UDDOM MVS Domain Names	64
UDEXAL MVS Exception Analysis Default Level Sets	65
UDCVNUM IDMS/CV Numbers	66
UDIJOBS IDMS Jobname Lists	66
UDIJOBS Macro Options	67
UDIDX1 IDMS Exception Analysis Default Level	67

You must review PreAlert macros during the installation process to determine the appropriate options for the data center. Although you will not alter the macro source code, these macros have default assignment values that require your attention and selection. Values for these macros are defined in the USERDATA member of the dataset `xxxx.PREALERT.CNTL`, where `xxxx` is your site's PreAlert high-level qualifier.

The following sections describe these macros, give valid keyword values, and provide the default value. The macros described are UDPARMS, UDAUSER, UDPGN, UDDOM, UDEXAL, UDCVNUM, UDIDXL, UDLCX, UDIJOBS, and UDCHATT.

UDPARMS PreAlert User Installation Data

The UDPARMS macro allows you to define numerous general options for the PreAlert system. The following text includes:

- Examples of UDPARMS macro definitions in the USERDATA member (one example each for the PreAlert/TSO and PreAlert/VTAM environments).
- A cross reference table that categorizes each UDPARMS macro keyword by function and provides a page reference for more detailed information on that keyword.
- Descriptions of each UDPARMS macro keyword.

UDPARMS Macro Example for PreAlert/TSO Userdata Options

[Figure 8](#) shows an example UDPARMS macro definition for a PreAlert system with user interface running in the TSO/ISPF environment.

Figure 8 • UDPARMS macro definition—TSO/ISPF environment

```

-----+-----1-----+-----2-----+-----3-----+-----4-----+-----5-----+-----6-----+-----7-----+-----8
      UDPARMS  PIDMS=PRODIDMS,           Production IDMS = PRODIDMS      X
                TIDMS=TESTIDMS,          Test IDMS = TESTIDMS       X
                RMF=Y,                   RMF used for MVS statistics  X
                MTSOID=MTSO,             PreAlert/TSO interface = MTSO  X
                HELPDSN=*.SHOPMON.HELP,  Screens file DSN mask       X
                MLOGDSN=*.PREALERT.MLOG, Statistics Logging DSN      X
                SPFLPA=Y,                 SPF in LPA                 X
                UNIT=SYSDA,               Default Dynamic Alloc unit   X
                CHECK=YES

```

UDPARMS Macro Example for PreAlert/VTAM Userdata Options

[Figure 9](#) shows an example UDPARMS macro definition for a PreAlert system with user interface running in a VTAM environment.

Figure 9 • UDPARMS macro definition—VTAM environment

```

-----+-----1-----+-----2-----+-----3-----+-----4-----+-----5-----+-----6-----+-----7-----+-----8
      UDPARMS  PIDMS=PRODIDMS,      Production IDMS = PRODIDMS      X
              TIDMS=TESTIDMS,      Test IDMS = TESTIDMS      X
              RMF=Y,                RMF used for MVS statistics  X
              MTSOID=MTSO,          PreAlert/TSO interface = MTSO  X
              HELPDN=* .SHOPMON.HELP, Screens file DSN mask      X
              MLOGDSN=* .PREALERT.MLOG, Statistics Logging DSN    X
              SPFLPA=Y,             SPF in LPA                    X
              UNIT=SYSDA,           Default Dynamic Alloc unit    X
              AUTHXIT=N,            All auth users in SHOPMAUS    X
              SECINT=Y,             Secure Auto-Update Option     X
              SECSAVE=N,            Do not secure Screen Save     X
              SECWAIT=Y,            Secure Wait Analysis          X
              VTAMMAX=4,            Max VTAM users = 4            X
              VTIME=900,            VTAM timeout interval=15 min  X
              VHOLD=N,              VTAM timeout = no hold        X
              CHECK=YES

```

Note:

Any specification for UDPARMS should begin in column 10. Keywords on additional lines should begin in column 16. The X in column 72 indicates a continuation of the line.

UDPARMS Option Cross-reference

Because of the number of UDPARMS macro options, the following table provides a concise list of the option keywords by function. Included in this table is a reference to the page where the option is described in detail.

User Authorization and Security Options

Keyword	Description	Page
SECINT	Restricted Auto-update option use (Y/N)	48
SECWAIT	Restricted Wait Analysis use (Y/N)	49
SECSAVE	Restricted Screen Save option use (Y/N)	49
AUTHXIT	User Security Exit call upon signon (Y/N)	49
AUTOATH	Authorization at signon for authorized users (Y/N)	49
AMVS	Types of line commands to which security applies	50

Print Options

Keyword	Description	Page
PRTCLS	Default SYSOUT class	51
PRTDEST	Default SYSOUT destination	51
PRTHOLD	Default SYSOUT hold attribute	51

Message Options

Keyword	Description	Page
WTORTC	Default WTO route codes	51
WTODSC	Default WTO descriptor codes	51
COMDWTO	Messages to master console for COMD command (Y/N)	51

Statistics Logging Options

Keyword	Description	Page
MLOGSMF	SMF record ID for logging	51
MLOGDSN	Default dataset name for statistics logging	51
MLOGDSP	Default disposition for existing logging dataset	52
MLOGBUF	Maximum buffer size for statistics logging	52
MLOGMEM	Help file member with JCL to offload MLOG datasets	52

Color and Highlighting Options

Keyword	Description	Page
PLOTYEL	Threshold for YELLOW highlighting on plots	52
PLOTRED	Threshold for RED highlighting on plots	52
COPN	Specifies color and highlighting attributes for normal PreAlert data displays	52
COPH	Specifies color and highlighting attributes for PreAlert messages and exception data	52
COUN	Specifies color and highlighting attributes for PreAlert line commands	52
COUH	Specifies color and highlighting attributes for PreAlert command input and blank lines	53
COIN	Specifies color and highlighting attributes for PreAlert line command input areas	53

Miscellaneous Options (of General Scope)

Keyword	Description	Page
AREP	Auto-repeat Option Indicator (Y/N)	53
TSO	Access method for TSO terminal I/O	53
HELPDSN	Dataset name mask for each user's screen file	53
MEMREP	Confirmation of user screen file replacement (Y/N)	53
SCRNLIM	Maximum # of screen names for SCRNL command	53
NOSAVE	Suppression of SAVE option (Y/N)	54
UNIT	Default unit name for dynamic allocation requests	54
INT	Auto-update interval control parameters	54
SPFLPA	ISPF modules in the Link Pack Area (LPA) (Y/N)	54
CHECK	UDPARMS macro syntax check for commas between the specified UDPARMS keywords (Y/N)	54
MENUHDR	Specifies display of the menu header Menus Active: at the top of each screen (Y/N)	54
CENDATE	Displays century date format, CYY.DDD. (Y/N)	55

IDMS Options

Keyword	Description	Page
PIDMS	Jobname for production IDMS CV JCL	55
TIDMS	Jobname for test IDMS CV JCL	55
IDMSMAX	Maximum # of CVs to be displayed per screen	55
IDMSRCE	Indicator of IDMS RCE analysis functionality	55
ITIME	Maximum number of seconds for CV log and journal allocations, opens, reads	55
IJRNLC	Minimum number of seconds between reads of IDMS journal header records	56
IJRNLF	Journal allocated and opened for each read (Y/N)	56
DCLOG	Read of IDMS log area for log-area-full percentage (Y/N)	56
IDMSSRB	Schedule SRB to monitor swapped out CVs (Y/N)	56
IDXPFX	Exception Analysis message ID prefix	56
IDXDATE	Inclusion of data in exception messages (Y/N)	56
IABXBY	Bypass ABXabend request check for TCENABN	56
IERRSND	Terminal beep option for IDMS interface errors.	57
IADS2	Name of Exception Analysis task code for ADSO	57
ILOGINT	Duration (minutes) for PreAlert interval statistics	57
ILOGSYN	Synchronization of interval statistics (Y/N)	57
ILOGSTA	Statistics logging for each statistics interval (Y/N)	57
ITASKST	Message for no task statistics collection (Y/N)	57
IDMSJCT	Maximum number of concurrent IDMS CVs	57
IUSMAX	Maximum number of user sessions per 12.0 CV	58
SPYIAT	.SPY screen name for IDMS active task data	58
SPYIRU	.SPY screen name for IDMS run unit data	58
SPYIBF	.SPY screen name for IDMS buffer data	58
SPYIDB	.SPY screen name for IDMS database area data	58
SPYIFC	.SPY screen name for IDMS file data	58

MVS Options

Keyword	Description	Page
RMF	RMF use for DASD, tape, page/swap dataset statistics (Y/N)	58
EXAPFX	Exception Analysis message ID prefix	59
EXADATE	Date for Exception Analysis messages (Y/N)	59
SPYMAS	.SPY screen name for MVS address space data	59
SPYMDD	.SPY screen name for MVS DASD device data	59

VTAM Options

Keyword	Description	Page
VAPPL	PreAlert VTAM application ID	59
VPASS	VTAM password for VTAM application ID	59
VTAMMAX	Maximum number of concurrent PreAlert/VTAM sessions allowed	59
VSNAPC	SYSOUT class for SNAP file	59
VSNAPH	Hold request for SNAP file abend	59
VTIME	User session timeout interval (seconds)	59
VHOLD	Session held internally on timeout (Y/N)	59
VAUTO	VTAM session timeout Auto-update option	60
VDATA	Logon data acceptance from VTAM logon screen	60
VSWAP	PreAlert/VTAM swappable operation (Y/N)	60
LU0SIZE	Maximum request unit size for LU type 0 terminals	60

TSO Options

Keyword	Description	Page
MTSOID	Interface ID for PreAlert/TSO	60
MTSOTIM	Look-around time for PreAlert/TSO logon requests	60
MTIME	MTSO session timeout interval (seconds)	60
MHOLD	MTSO session held after timeout (background)	60
MAUTO	MTSO session timeout auto-update option	60

PreAlert ASG-Server Facility Options

Keyword	Description	Page
ASFID	Subsystem ID for the ASG-Server Facility	61
ASFFUN	Name of ASG-Server Facility function for exception messages	61

ASG-SIRF Local Mode Options

Keyword	Description	Page
SIRFLME	Maximum number of Local Mode Elements that can be monitored simultaneously	58
SPYSLM	.SPY screen name for ASG-SIRF local mode data	58

UDPARMS Option Descriptions

The UDPARMS macro options are described in the subsections within this section.

User Authorization and Security Options

SECINT

Specifies whether only PreAlert authorized users have use of the Auto-update option. Valid values:

Y (default)

Only PreAlert authorized users have access to the Auto-update option.

N

All PreAlert users have access to the Auto-update option.

SECWAIT

Specifies whether only PreAlert authorized users have use of the PreAlert Wait Analysis function. Valid values:

Y (default)

Only PreAlert authorized users have access to the Wait Analysis function.

N

All PreAlert users have access to the Wait Analysis function.

SECSAVE

Specifies whether only PreAlert authorized users have use of the PreAlert Screen Save option. Valid values:

Y (default)

Only PreAlert authorized users have access to the Screen Save option.

N

All PreAlert users have access to the Screen Save option.

AUTHXIT

Specifies whether the User Security Exit will be called when a user signs on and the user's ID has not been included in the UDAUSER macro. Valid values:

N (default)

Do not call the User Security Exit.

Y

Call the User Security Exit.

AUTOATH

Specifies whether authorization will be turned on automatically at signon for PreAlert authorized user IDs. Valid values:

Y (default)

Authorization will be automatically turned on.

N

Authorization will not be automatically turned on. The .AUTHON or .ATH ON command must be used to turn on authorization.

AMVS

Specifies the types of PreAlert/MVS line commands to be secured. Multiple types may be specified, for example, `AMVS=(DUMP,MCON,MVSS)`. Multiple values must be separated by commas and enclosed within a single set of parentheses. Refer to ["AMVS Security Facility" on page 80](#) for further information on this command. Valid values:

NONE (default)

No additional security to be added for PreAlert.MVS.

ASID

Address Space Data, Address Space Trace commands.

DISK

Disk Device Analysis, Disk Trace commands

TAPE

Tape Device Analysis commands

SYST

MVS System Analysis, CPU Utilization, Page/Swap Datasets, SRM Displays, Real Storage, CSA/SQA Usage

DUMP

Storage Display and Modification

MCON

Master Console Support

MVSS

MVS System Services

EXA

MVS Exception Analysis

DSN

Dataset Displays

ALL

All of the above types.

Print Options

PRTCLS

Specifies the default SYSOUT class for print function requests (default=A).

PRTDEST

Specifies the default SYSOUT destination for print function requests (default=R0).

PRTHOLD

Specifies the default SYSOUT hold attribute for print function requests. Valid values are N (default) or Y.

Message Options

WTORTC

Specifies the default WTO Route Codes for all WTOs issued by PreAlert. Valid values range from 1 through 16 (default=11). Multiple values must be separated by commas and enclosed within a single set of parentheses, e.g., WTORTC=(2,11). For further information on route codes, refer to the IBM MVS Message Library, Routing, and Descriptor Codes publication.

WTODSC

Specifies the default WTO Descriptor Codes for all WTOs issued by PreAlert. Valid values range from 1 through 16 (default=7) and must be enclosed within a single set of parentheses. Multiple descriptor codes may be specified, e.g., WTODSC=(4,7). For further information on descriptor codes, refer to the IBM MVS Message Library, Routing, and Descriptor Codes publication.

COMDWTO

Specifies whether audit messages will be directed to the master console when the PreAlert COMD line command is issued. Valid values are Y (default) or N.

Statistics Logging Options

MLOGSMF

Specifies the SMF record ID to be used for statistics logging to SMF. Must be in the range from 128 through 255 (default=000).

MLOGDSN

Specifies the default name of the dataset to be used for statistics logging. An asterisk (*) anywhere in the dataset name will be replaced with the user ID of the PreAlert user requesting statistics logging. There is no default.

MLOGDSP

Specifies the default disposition to be used for allocating an existing dataset for statistics logging. OLD and SHR may also be specified. New datasets dynamically allocated for statistics logging are allocated with DISP=MOD (default=MOD).

MLOGBUF

Specifies the maximum buffer size allowed for statistics logging. The size is specified in bytes (default=204800).

MLOGMEM

Specifies the name of the PreAlert Help file member that contains JCL to offload the MLOG datasets (default=#MLOGOFF). Refer to ["1.6 Initializing Statistics Logging" on page 14](#).

Color/Highlighting Options

PLOTYEL

Specifies the threshold beyond which plots will be displayed in yellow, if color support has been activated (default=30).

PLOTRED

Specifies the threshold beyond which plots will be displayed in red, if color support has been activated (default=70).

COPN

Specifies color and highlighting attributes for normal PreAlert data displays. Values must follow the syntax (*color, highlight*) and are described as follows:

color

Screen color, valid values are RED, BLUE, TURQ, YELLOW, WHITE, GREEN, PINK

highlight

Highlighting attribute, valid values are NORMAL, USCORE, REVERSE, BLINK

COPH

Specifies color and highlighting attributes for PreAlert messages and exception data. Values must follow the syntax (*color, highlight*) and are described with the COPN keyword.

COUN

Specifies color and highlighting attributes for PreAlert line commands. Values must follow the syntax (*color, highlight*) and are described with the COPN keyword.

COUH

Specifies color and highlighting attributes for PreAlert command input and blank lines. Values must follow the syntax (*color, highlight*) and are described with the COPN keyword.

COIN

Specifies color and highlighting attributes for PreAlert line command input areas. Values must follow the syntax (*color, highlight*) and are described with the COPN keyword.

Miscellaneous Options (of General Scope)

AREP

Specifies whether the PreAlert Auto-repeat option will be active to provide for overflow display conditions on selected line commands. Valid values:

Y (default)

Auto-repeat option active.

N

Auto-repeat option inactive.

TSO

Specifies the access method for TSO terminal input and output. Valid values are VTAM (default) or TCAM.

HELPDSN

Specifies the name mask of the dataset allocated for each user's screen file. In the mask, any asterisk (*) will be replaced by the user's ID (default=
* . PREALERT . HELP).

MEMREP

Specifies whether the user will be prompted to confirm the replacement before any existing screen member is replaced in the user's PreAlert help file. This option provides a safeguard against accidentally replacing a user-defined screen format. Valid values:

Y (default)

The user will be prompted before the screen member is replaced.

N

The screen member will be replaced without the user being prompted.

SCRNLIM

Specifies the maximum number of screen names maintained for the SCRNL line command display (default=512). This option does not affect the number of screens that can be defined by PreAlert users.

NOSAVE

Specifies whether the SAVE option will be suppressed. Valid values:

N (default)

Does not suppress the SAVE option.

Y

Suppresses the SAVE option for all users. This value should be used if the HELPDSN keyword does not include the asterisk to generate a unique dataset name for each user.

UNIT

Specifies the default unit for all Dynamic Allocation Requests (default= SYSDA).

INT

Specifies values for Auto-update Interval Control. Values must follow the syntax (*a*, *b*, *c*) and are described as follows:

a

Default Auto-update Interval (default=5).

b

Minimum interval for non-authorized users (default=3).

c

Auto-update time limit for non-authorized users (default=600).

SPFLPA

Specifies whether the ISPF modules reside in the Link Pack Area (LPA). Valid values are Y (default) or N.

CHECK

(PreAlert internal use only—must be the last UDPARMS keyword specified in the USERDATA member.) Value must always be YES. If a comma is omitted after any of the UDPARMS keyword values, the value of this keyword defaults to NO and, consequently, the UDPARMS macro will fail.

MENUHDR

Specifies whether the menu header **Menus Active:** is to be displayed at the top of each screen. The Menu header displays the status of the Menu stack.

Y (default)

The menu header is displayed at the top of the screen.

N

The menu header is not displayed.

CENDATE

Normally, PreAlert displays the Julian date using the YY.DDD format. With CENDATE=Y, the Julian date displays using the CYY.DDD format where C is the century bit. January 1, 2000 displays as 100.001, the century bit being set to 1 beginning with the year 2000.

IDMS Options**PIDMS**

Specifies the jobname for the production IDMS CV (default=PRODIDMS). This name will replace the PRODIDMS jobname, found in the PreAlert pre-defined menus and tutorial screens. Refer to the *ASG-PreAlert IDMS User's Guide*.

TIDMS

Specifies the jobname for the test IDMS CV. This name will replace the TESTIDMS jobname, found in the PreAlert pre-defined menus and tutorial screens.

IDMSMAX

Specifies the maximum number of IDMS CVs for which statistics will be displayed on any given screen (default=4). Any number above 4 will increase the amount of storage PreAlert uses and could affect the performance of PreAlert. For PreAlert under Local (native) TSO, the user's TSO region size also would need to be increased.

IDMSRCE

Controls IDMS RCE analysis as follows:

Y

Performs RCE analysis for storage size and RCE count for user (online) and external tasks only, but not for system tasks.

N (default)

Suppresses IDMS RCE analysis for active task storage size and RCE count (ASTA and ATRE line commands).

S

Performs RCE analysis for storage size and RCE count for all tasks: system, user, and external.

ITIME

Specifies the number of seconds (default=20) to wait for allocation, open, and read for the IDMS CV Log area and Journal files. PreAlert will abend (User 600) when this limit is reached.

IJRNL

Specifies the minimum time interval between IDMS Journal Header Record reads in number of seconds (default=0). Zero seconds specifies that Journal Header Records will be read with each PreAlert update. Negative one seconds specifies that no Journal Header Records will be read. Refer to the *ASG-PreAlert User's Guide*.

IJRNLF

Specifies whether PreAlert will open and allocate the IDMS journal files. Valid values:

N (default)

PreAlert will allocate and open the journal files once and will retain the allocation until PreAlert is stopped or until PreAlert detects that the CV has been stopped.

Y

PreAlert will allocate, open, read, close, and de-allocate the journal files for each journal read. The journal read interval (IJRNL) must be 60 seconds or more.

DCLOG

Specifies whether PreAlert will allocate and read the IDMS log area to obtain log-area-full percentages. Refer to "PreAlert and IDMS DC Log" in the *ASG-PreAlert IDMS User's Guide*.

IDMSSRB

Specifies how PreAlert will monitor swapped-out IDMS CVs. Valid values are Y (default) or N. Refer to "Monitoring Swappable CVs" in the *ASG-PreAlert IDMS User's Guide*.

IDXPFX

Specifies the message ID prefix used when Exception Analysis sends a message to either the console or TSO users (default=SMIDX). The prefix must be five characters long.

IDXDATE

Specifies whether the date will be included in exception messages sent to the console or to TSO users. Valid values are Y (default) or N.

IABXBY

Specifies the bypass of the TCENABN check when the ABX option in IDMS Active Task Exception Analysis requests that a task abend. The TCENABN is a flag in the Task Control Element (TCE) that indicates "DON'T ALLOW ABEND IF ON." With IABXBY=N (default), the TCENABN flag is checked before the ABX abend request is processed and if TCENABN is set, then the abend request is denied. With IABXBY=Y, the TCENABN check is bypassed and the abend request is processed regardless of the TCENABN flag.

IERRSND

Requests the terminal sound (beep) option if a condition exists that prevents PreAlert from monitoring the IDMS CV. The conditions included are IDMS jobname not found, invalid IDMS jobname, IDMS init incomplete, IDMS-CV being shutdown, job swapped out, and IDMS common system area not found. IERRSND=Y will request the terminal sound options when one of these conditions are displayed by the IDMS line command.

IADS2

Specifies, for Exception Analysis task codes, the name of the task code used to execute ADSO processes (default=ADS2) .

ILOGINT

Specifies the duration (in minutes) for PreAlert interval statistics (default=15) . Refer to "IDMS Statistics Intervals" in the *ASG-PreAlert User's Guide*.

ILOGSYN

Specifies whether PreAlert (IDMS) interval statistics should be synchronized. Valid values:

N (default)

Do not synchronize PreAlert interval statistics.

Y

Synchronize PreAlert interval statistics. The value of the ILOGINT keyword should be 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, or 60.

ILOGSTA

Specifies whether PreAlert (IDMS) interval statistics will be written at the end of each statistics interval. Valid values are N (default) or Y. For further information, refer to the *ASG-PreAlert IDMS User's Guide*.

ITASKST

Specifies whether PreAlert will check to see that task statistics are being collected in the IDMS CV. Valid values:

Y (default)

Verification will be done. If task statistics are not being collected, the message `Task statistics not available` will appear after any IDMS line command issued on a PreAlert display.

N

Checking will be suppressed.

IDMSJCT

Specifies the maximum number of concurrent IDMS CVs in the system (default=64) . It does not affect the number of CVs that PreAlert can monitor.

IUSMAX

Specifies the estimated maximum number of user sessions running per IDMS CV (default=256). This figure is the maximum number of entries for the Lock Summary Table. Refer to the *ASG-PreAlert IDMS User's Guide*.

SPYIAT

Specifies the .SPY screen name for IDMS active task data (default=SPYIAT). This screen allows the user to spy on an IDMS active task. Refer to the *ASG-PreAlert IDMS User's Guide*.

SPYIRU

Specifies the .SPY screen name for IDMS run unit data (default=SPYIRU). This screen allows the user to spy on an IDMS run unit.

SPYIBF

Specifies the .SPY screen name for IDMS buffer data (default=SPYIBF). This screen allows the user to spy on an IDMS buffer.

SPYIDB

Specifies the .SPY screen name for IDMS database area data (default=SPYIDB). This screen allows the user to spy on an IDMS database area.

SPYIFC

Specifies the .SPY screen name for IDMS file data (default=SPYIFC). This screen allows the user to spy on an IDMS file.

ASG-SIRF Options

SIRFLME

Specifies the maximum number of ASG-SIRF Local Mode Elements that PreAlert can monitor concurrently (default=16). When the total number of 10.2 run units or 12.0 local mode transactions exceeds this limit, PreAlert will produce an error message indicating that some ASG-SIRF Local Mode Elements are not being monitored.

SPYSLM

Specifies the .SPY screen name for ASG-SIRF local mode data (default=SPYSLM). This screen allows the user to spy on an ASG-SIRF Local Mode Element.

MVS Options

RMF

Specifies whether RMF will be used to collect DASD, tape, and page/swap dataset statistics. Valid values are Y (default) or N.

EXAPFX

Specifies the message ID prefix for Exception Analysis messages sent to either the console or TSO users (default=PAEXA). This prefix must be five characters long.

EXADATE

Specifies whether the date will be included in exception messages sent to the console or TSO users. Valid values are N (default) or Y.

SPYMAS

Specifies the .SPY screen name for MVS address space data (default=SPYMAS) . This screen allows the user to spy on an MVS address space. Refer to the *ASG-PreAlert IDMS User's Guide*.

SPYMDD

Specifies the .SPY screen name for MVS DASD device data (default=SPYMDD) . This screen allows the user to spy on DASD devices being accessed through MVS.

VTAM Options

VAPPL

Specifies the PreAlert VTAM application ID to be used if PreAlert is being executed via VTAM (default=PREALERT). Refer to ["Step 2 - Installing PreAlert/VTAM" on page 21](#) for more information.

VPASS

Specifies the VTAM password associated with the VTAM application ID (VAPPL). (Default=PREALERT).

VTAMMAX

Specifies the maximum number of concurrent PreAlert/VTAM sessions allowed (default=4).

VSNAPC

Specifies the SYSOUT class for the SNAP file (ABEND dumps) allocated for each user session (default=A).

VSNAPH

Specifies whether HOLD=YES will be requested for the SNAP file (ABEND dumps) allocated for each user session. Valid values are Y (default) or N.

VTIME

Specifies the PreAlert/VTAM session timeout interval in seconds (default=900). Also see the explanations for the VHOLD and VAUTO options below.

VHOLD

Specifies whether the session will be held (switched to background) when a PreAlert/VTAM session times out. Valid values are Y (default) and N.

VAUTO

Specifies the Auto-update option for sessions held after a PreAlert/VTAM session times out. VHOLD=Y is required. Valid values are Y and N (default).

VDATA

Specifies whether PreAlert/VTAM will accept VTAM logon data. Valid values are:

Y (default)

PreAlert/VTAM will accept log-on data from LOGON APPLID(applid) DATA (user ID/password, screen).

N

PreAlert/VTAM will ignore all log-on data. This value is recommended when type 0 logical units may be used.

VSWAP

Specifies whether PreAlert/VTAM will run swappable. Valid values are Y (default) or N.

LU0SIZE

Specifies the maximum request unit (RU) size for LU-type 0 terminals (default=1024). Since the VTAM Large Message Processing Enhancement option is not supported for LU-type 0 terminals, PreAlert must split large screens into request units not larger than the maximum size specified.

TSO Options

MTS0ID

Specifies a four-character interface ID for PreAlert/TSO (default=*). An asterisk (*) suppresses initialization of the PreAlert/TSO Interface. Refer to ["2.6 Specifying Userdata Options" on page 22](#).

MTS0TIM

Specifies the look-around time for PreAlert/TSO logon requests (default=3). A lower value would shorten response time for logons, but increase CPU overhead.

MTIME

Specifies the PreAlert/TSO session timeout interval in seconds (default=0). Also see the explanations for MHOLD and MAUTO options below.

MHOLD

Specifies whether sessions will be held (switched to background) when a PreAlert/TSO session times out. Valid values are Y and N (default).

MAUTO

Specifies the Auto-update option for sessions held after a PreAlert/TSO session times out. MHOLD=Y is required. Valid values are Y and N (default).

ASG-SERVER FACILITY Options

ASFID

Specifies the default four-character subsystem ID for ASG-Server Facility for the appropriate platform. (There is no default). This value is used when an exception definition specifies an equals sign (=) for the server ID. Refer to the chapter on Exception Analysis in the *ASG-PreAlert IDMS User's Guide*.

ASFFUN

Specifies the name of the ASG-Server Facility function used to process exception messages issued from PreAlert (default=EVENT.NOTIFICATION.FACILITY).

UDAUSER Authorized User IDs

The UDAUSER macro is used to specify authorized user IDs and their associated line command exclude lists (restricted command lists). One UDAUSER macro definition must be specified in the USERDATA member for each PreAlert authorized user as shown in [Figure 10](#).

Figure 10 • UDAUSER macro definition

```

-----+-----1-----+-----2-----+-----3-----+-----4-----+-----5-----+-----6-----+-----7-----+-----8
UDAUSER  USERID1
UDAUSER  USERID2
UDAUSER  USERID3, LCX=(LCXMZAP)
UDAUSER  USERID4, LCX=(LCXCOMD, LCXMZAP)
UDAUSER  USERID5, IJOBS=(IDMSJ1, IDMSJ2)
UDAUSER  USERID6, IJOBS=(IDMSJ1, IDMSJ2), LCX=(LCXMZAP)

```

UDAUSER Macro Options

The text in this section describes each option for the UDAUSER macro.

user ID

Specifies the ID of the PreAlert authorized user.

LCX

References the line command exclude lists associated with the user ID. All specified line command exclude lists must be enclosed in a single set of parentheses. Definition of the exclude lists is given below in ["UDLCX Line Command Exclude Feature" on page 62](#). Refer to the *ASG-PreAlert IDMS User's Guide* for instructions on authorized user IDs.

IJOBS

References the IDMS jobname lists associated with the user ID. All specified IDMS jobname lists must be enclosed in a single set of parentheses. Definitions of IDMS jobname lists are given in ["UDIJOBS IDMS Jobname Lists" on page 66](#). Refer to "Default IDMS jobnames," in the *ASG-PreAlert IDMS User's Guide*, for instructions on using IDMS jobname lists.

User IDs may also be authorized via the PreAlert security exit. Refer to ["Security Considerations" on page 69](#) for a description of the security exit.

UDLCX Line Command Exclude Feature

The UDLCX macros are used to specify the Line Command Exclude lists referenced by the UDAUSER macro discussed in ["UDAUSER Authorized User IDs" on page 61](#). One UDLCX macro must be defined in the USERDATA member for each exclude list. [Figure 11](#) lists an example.

Figure 11 • UDLCX macro

```
-----1-----2-----3-----4-----5-----6-----7--
LCXMVS   UDLCX  LCX=(APFL,CMDA,KILL,LPAM)
LCXCOMD  UDLCX  LCX=(COMD)
```

UDLCX Macro Options

The text in this section describes each option for the UDLCX macro options.

list-name

Specifies the name associated with the line command exclude list. This name is specified to the left of the UDLCX macro name.

LCX

Specifies one or more secured line commands or functions. Multiple command names must be separated by commas and enclosed within a single set of parentheses. Refer to PreAlert ["Security Considerations" on page 69](#) for further information.

UDCHATT Special Character Attributes

The UDCHATT macro defines the special character attributes used in comment displays. These special characters allow the user to add color and highlighting to the comments and menus.

Each UDCHATT macro specifies a single special character and assigns the intensity for monochrome displays and color and highlighting attributes. [Figure 12](#) gives an example.

Figure 12 • UDCHATT macro example

```

-----1-----2-----3-----4-----5-----6-----7--
UDCHATT CHAR=@, INTENS=LOW, COLOR= (YELLOW, NORMAL)
UDCHATT CHAR=#, INTENS=HIGH, COLOR= (WHITE, USCORE)

```

UDCHATT Macro Options

The text in this section describes each option for the UDCHATT macro.

CHAR

Specifies the specific character being defined.

INTENS

Specifies the intensity level. Valid intensities are LOW and HIGH.

COLOR (*color*, *highlight*)

Specifies the color and highlight in parentheses, using the following syntax. Valid colors are RED, BLUE, TURQ, YELLOW, WHITE, GREEN, and PINK. Valid highlights are NORMAL, USCORE, REVERSE, and BLINK.

UDPGN MVS Performance Group Names

The UDPGN macro allows the user to assign names to performance groups. These names are displayed by PreAlert.MVS for address space data and CPU and paging activity summaries. One UDPGN macro must be defined in the USERDATA member for each performance group. [Figure 13](#) lists an example.

Figure 13 • UDPGN macro example

```

-----1-----2-----3-----4-----5-----6-----7--
UDPGN 0, SYSTEM
UDPGN 1, TEST-BAT

```

UDPGN Macro Options

The text in this section describes each option for the UDPGN macro.

`n`

Specifies the number identifying the performance group.

`description`

Specifies an eight-character description of the performance group. This description is user defined and contains no blank characters.

UDDOM MVS Domain Names

The UDDOM macro allows the user to assign names to MVS domains. These names are displayed by PreAlert.MVS for address space data and CPU and paging activity summaries. One UDDOM macro must be defined in the USERDATA member for each domain. [Figure 14](#) lists an example.

Figure 14 • UDDOM macro example

```
-----+-----1-----+-----2-----+-----3-----+-----4-----+-----5-----+-----6-----+-----7-----+-----8
      UDDOM 0,SYSTEM
      UDDOM 1,TEST-BAT
```

UDDOM Macro Options

The text in this section describes each option for the UDDOM macro.

`n`

Specifies the number identifying the domain.

`description`

Specifies an eight-character description of the domain. This description is user-defined and contains no blank characters.

UDEXAL MVS Exception Analysis Default Level Sets

The UDEXAL macro assigns default MVS Exception Analysis level sets. Each level set specifies a threshold that defines exception conditions. The default level set is loaded automatically when the PreAlert.MVS interface is initialized. The default level sets are assigned by PreAlert user ID and MVS system ID. One UDEXAL macro must be defined in the USERDATA member for each user or group of users. [Figure 15](#) lists an example.

Figure 15 • UDEXAL macro example

```

-----1-----2-----3-----4-----5-----6-----7-----8
      UDEXAL USR=USER1,EXA=(MVS1,11,MVS2,12)
      UDEXAL USR=USER2,EXA=(MVS1,21,*,29)
      UDEXAL USR=*,EXA=(MVS1,91,MVS2,92,*,99)

```

In the example, MVS Exception Analysis level sets are assigned by user ID and MVS system ID as follows:

MVS System user ID	MVS1	MVS2	Other
USER1	11	12	99
USER2	21	29	29
OTHERS	91	92	99

By using the PreAlert user IDs, separate level set defaults may be maintained for different PreAlert users. Additionally, the MVS system ID allows for separate defaults when PreAlert is shared across multiple MVS systems.

UDEXAL Macro Options

The text in this section describes each option for the UDEXAL macro.

USR

Specifies the PreAlert user ID associated with the level set. An asterisk (*) is specified to define the level set defaults for any user IDs not specified in any of the UDEXAL macro definitions. Must always be specified in each UDEXAL macro definition. There is no default.

EXA

Specifies the list of MVS system IDs and their default MVS Exception Analysis Level Sets. The specified system IDs and level sets must be separated by commas and enclosed within a single set of parentheses. An asterisk (*) may be used for the system ID to indicate the default level set for any system IDs not specified in the given UDEXAL macro definition. There is no default.

UDCVNUM IDMS/CV Numbers

The UDCVNUM macro allows the user to use the IDMS CV number rather than the jobname with the IDMS line command. One UDCVNUM macro must be defined in the USERDATA member for each CV. [Figure 16](#) lists an example.

Figure 16 • UDCVNUM macro example

```

-----+-----1-----+-----2-----+-----3-----+-----4-----+-----5-----+-----6-----+-----7-----+-----8
UDCVNUM 1, IDMSPROD
UDCVNUM 90, IDMSDEVL

```

UDCVNUM Macro

The text in this section describes each option for the UDCVNUM macro:

n

Specifies the CV number.

jobname

Specifies the jobname for the CV JCL. Refer to "Selecting IDMS CV Names by Number" in the *ASG-PreAlert IDMS User's Guide*.

UDIJOBJS IDMS Jobname Lists

The UDIJOBS macro builds a list of IDMS jobnames to be used when PreAlert encounters an IDMS line command without a jobname. For details on how PreAlert selects the IDMS jobname, refer to "Default IDMS jobnames," in the *ASG-PreAlert IDMS User's Guide*.

PreAlert only selects a single IDMS jobname list for the user based upon the SMF system ID the user is running under. A system ID may be specified with the jobname list. If the system ID is specified, PreAlert only uses the list if the system ID matches the SMF system ID that you are currently running under. If a system ID is not specified, PreAlert selects the list only when PreAlert did not find a list with a matching system ID.

Figure 17 • IDMS jobname lists

```

-----+-----1-----+-----2-----+-----3-----+-----4-----+-----5-----+-----6-----+-----7-----+-----8
IDMSJ0  UDIJOBS  IJOBS=(IDMS01, IDMS02)
IDMSJ1  UDIJOBS  SYS=MVS1, IJOBS=(IDMS11, IDMS12, IDMS13, IDMS14)
IDMSJ2  UDIJOBS  SYS=MVS2, IJOBS=(IDMS21, IDMS22, IDMS23, IDMS24)

```

UDIJOBS Macro Options

The text in this section describes the each options for the UDIJOBS macro.

label

Specifies a name for the IDMS jobname list. This name is used in the UDAUSER macro to associate the list with the user ID.

SYS

Specifies the optional system ID for the jobname list. PreAlert will only use the list if the system ID matches the SMF system ID for the system that PreAlert is being executed.

IJOBS

Specifies the list of IDMS jobnames. The assembler limits the list of jobnames to 255 characters, including commas and parentheses. This imposes a practical limit of 28 8-character jobnames. If more than 28 jobnames are required, the IJOBS2 and IJOBS3 keywords may also be used.

Refer to, "Default IDMS Jobnames" in the *ASG-PreAlert IDMS User's Guide*, for specifics on how PreAlert selects the IDMS jobnames.

IJOBS2

Specifies a second list of IDMS jobnames.

IJOBS3

Specifies a third list of IDMS jobnames.

UDIDXL IDMS Exception Analysis Default Level

The UDIDXL macro is used to associate default IDMS Exception Analysis level sets with specific IDMS jobnames. The default level set will be loaded automatically when PreAlert begins monitoring the CV.

A list of IDMS jobnames and level sets is built for a specific PreAlert user ID. This allows different user IDs to maintain separate lists. Also, a global list may be specified, which is used for user IDs and jobnames not specified in any of the UDIDXL macro definitions. [Figure 18](#) lists an example.

Figure 18 • UDIDXL macro definition example

```

-----1-----2-----3-----4-----5-----6-----7-----8
UDIDXL USR=USER1,IDX=(IDMSCV1,11,IDMSCV2,12)
UDIDXL USR=USER2,IDX=(IDMSCV1,13,IDMSCV4,17)
UDIDXL USR=*,IDX=(IDMSCV1,14,IDMSCV2,15,IDMSCV3,16)

```

From the example, the Exception Analysis level sets are assigned by user ID and jobname as follows:

Jobname User ID	IDMSCV1	IDMSCV2	IDMSCV3	IDMSCV4
USER1	11	12	16	NONE
USER2	13	15	16	17
OTHERS	14	15	16	NONE

UDIDXL Macro Options

The text in this section describes each option for the UDIDXL macro.

USR

Specifies the PreAlert user ID to be associated with the level sets. An asterisk (*) is specified to indicate any user ID that has not been specified in any of the UDIDXL macro definitions.

IDX

Specifies the list of IDMS jobnames and their associated Exception Analysis level set. Jobnames and their level sets must be separated by commas and enclosed within a single set of parentheses.

5

Security Considerations

This chapter covers these topics:

Security Features	70
Default Security Features	70
Line Command Exclude Feature	71
Security Exit	72
Sample Security Exits	74
Secured Line Commands and Functions	77
IDMS Interface	77
Storage Display and Modification	77
Master Console Support	78
MVS System Services	78
Dataset Displays	79
Address Space Restricted Functions	79
Control Commands	79
MVS Wait Analysis	79
Authorized User IDs	80
SMF Logging	80
AMVS Security Facility	80
AMVS Secured Functions	81

Security Features

PreAlert's security features provide these types of security requests:

- User signons to PreAlert
- Authorized user IDs
- Secured line commands and functions

An authorized user ID is a basic security concept in PreAlert. An authorized user has the ability to turn on authorization via the .ATH line command or the .AUTHON control command. Once an authorized user has turned authorization on, then the user may access the secured line commands and functions listed later in this chapter. A user who is not authorized will not be allowed to turn on authorization or to access the secured line commands and functions.

Security may be implemented in three levels. Basic security is provided through the Default Security Features. Intermediate security is provided by the Line Command Exclude Feature. Full security is provided through the Security Exit interfaces. A security exit is provided for RACF. Users also can develop security exits for other security packages. Sample security exits are provided that may be tailored for such other security packages as CA-ACF2 and CA-TOP SECRET.

Default Security Features

Default security features are provided by a security exit that allows all security requests. The USEREXIT sample security exit, see ["USEREXIT Default Security Exit" on page 75](#) for the default security.

User Signons to PreAlert are not secured by the default features. The default security features allow any user to sign on to PreAlert. PreAlert does not attempt to validate either the user ID or password from the Signon screen.

Authorized User IDs must be specified in the userdata UDAUSER macro when the AUTHXIT=N keyword is specified in the UDPARMS macro. If AUTHXIT=Y has been specified, all user IDs are considered authorized.

Secured line commands and functions are available to any authorized user ID. An authorized user may use any of the secured line commands and functions.

Line Command Exclude Feature

The Line Command Exclude feature, LCX, provides a means of preventing authorized users from accessing secured line commands. In the userdata UDAUSER macro, each authorized user ID must be specified along with the names of one or more line command exclude lists. The userdata UDLCX macro is used to build the line command exclude lists. [Figure 19](#) lists a userdata sample.

Figure 19 • Userdata UDLCX macro example

```

-----+-----1-----+-----2-----+-----3-----+-----4-----+-----5-----+-----6-----+-----7-----+-----8
      UDPARMS AUTHXIT=N,          DONT CALL EXIT NON-AUTH USERID  X
              AMVS=(TAPE),        PA MVS SECURED FUNCTIONS      X
              PIDMS=PRODIDMS,      PROD IDMS JOB NAME=PRODIDMS    X
      .....
      UDAUSER USERID1
      UDAUSER USERID2
      UDAUSER USERID3,LCX=(LCXMZAP)
      UDAUSER USERID4,LCX=(LCXCOMD,LCXMZAP)
      UDAUSER USERID5,LCX=(LCXAMVS)
      ....
      LCXAMVS  UDLCX  LCX=(AMVS)
      LCXCOMD  UDLCX  LCX=(COMD,IVRY,ICMD)
      LCXMZAP  UDLCX  LCX=(MZAP,KEY0)

```

From the userdata sample above, only user IDs one through four (e.g., USERID1 through USERID5) are authorized. Only these users are able to access the secured line commands or functions. USERID1 and USERID2 have unrestricted access to all secured line commands and functions. USERID3 is restricted from the line commands and functions in the UDLCX macro for LCXMZAP. USERID4's access is restricted by LCXCOMD and LCXMZAP. USERID5's access is restricted from the AMVS secured functions by LCXAMVS.

User Signons to PreAlert are not secured by the line command exclude feature. Any user may signon to PreAlert. PreAlert will not validate the user ID or password from the Signon screen.

Authorized User IDs must be specified in the userdata UDAUSER macro.

AUTHXIT=N should also be specified in the UDPARMS macro. Each user ID may be restricted by one or more line command exclude lists.

Secured line commands and functions may be controlled through the UDLCX macros. A UDLCX macro defines a line command exclude list to prevent authorized user IDs from accessing the specified line commands and functions.

Security Exit

The security exit provides additional security for each of the three levels: user signons, authorized user IDs, and secured line commands and functions. In general, the exit is designed to control access for a few specific security requests and to allow all other requests. It is much easier for the exit to control access to a few specific requests than to explicitly control every request from PreAlert. The use of the exit for each level is described later in this section.

The exit communicates with PreAlert via register 1 containing the address of a parameter list.

PARM List	Description
+ 0	Name of line command or secured function (four characters)
+ 4	User ID (eight characters)
+ 12	PARM list extension address (four bytes)
+ 16	PARM list extension length (four bytes)

The format and contents of the parameter list extension depend upon the level of security being tested. All character data translates to capital letters only, no lower case. Other data, addresses, and lengths are in hexadecimal full words.

Actual validation of the security request may either be hard coded in the exit or passed to a security package such as RACF, ACF2, or Top Secret. Sample security exits are described in ["SAMPEXIT Sample Security Exit" on page 75](#).

The security exit must place a return code in register 15 to indicate whether the request is allowed or denied. A return code of 0 (zero) allows the request. A return code of 4 denies the request. A return code of 8 denies the request and indicates that the exit has provided a message to be displayed by PreAlert.

The address and length of the message are placed in PARM list extension address and length fields prior to returning to PreAlert.

User Signons to PreAlert may be controlled by the security exit. When the user signs on to PreAlert, the user ID, password, and Terminal ID are passed to the exit through the parameter list.

PARM List	Description
+ 0	C'MUSR' - User signon function

PARM List	Description
+ 4	user ID (eight characters)
+ 12	PARM list extension address
+ 16	16 (length of extension)

PARM List Extension	Description
+ 0	VTAM logical unit ID (PreAlert/VTAM only)
+ 8	Password (eight characters)

When the user signs off, the exit will be called again with the PARM list.

PARM List	Description
+ 0	C'SOFF' - User signoff function
+ 4	User ID (eight characters)
+ 12	0 (no extension)
+ 16	0

The signon and signoff functions may have specific requirements when a security package is invoked. Refer to ["SAMPEXIT Sample Security Exit" on page 75](#) for the particular security package your site is using.

Authorized User IDs must be specified in the userdata UDAUSER macro when AUTHXIT=N keyword is specified in the UDPARMS macro.

When AUTHXIT=Y has been specified, PreAlert checks the UDAUSER macro first. If the user ID was found in the UDAUSER macro, the user ID is considered authorized. If the user ID was not found, then the exit is called with this parameter list:

PARM List	Description
+ 0	C'AUTH' - User ID authorization request
+ 4	User ID (eight characters)
+ 12	0 (no extension)
+ 16	0

Secured line commands and functions are passed to the exit along with the user ID through the parameter list.

PARM List	Description
+ 0	Name of line command or function (four characters)
+ 4	User ID (eight characters)
+ 12	PARM list extension address
+ 16	PARM list extension length

PARM List Extension	Description
+ 0	Line command input

The PARM list extension is used to pass any input associated with the line command or function. If no input is available, the extension length field will contain hexadecimal zeros.

The exit may examine the user ID, line command, and input to determine if the request is to be allowed. For example, when the IDMS line command is used, the jobname of the IDMS CV (input to the line command), along with the user ID, is passed to the exit. The exit can limit the IDMS line command by the IDMS CV and/or the user ID.

Sample Security Exits

The following sample security exits are included in the PreAlert control file. JCL to assemble and link the exits is included in the ASMEXIT member. The exits should be considered as samples only; they may not fit your installation requirements.

Note: _____

Exits are provided as samples only. Any additional tailoring is the individual user's responsibility.

All security exits are assembled and linked as non-reentrant and non-reusable. This means that each PreAlert user will have a separate copy of the exit. Also, the exit can modify itself, allowing the exit to remember what has happened in the past.

When testing a security exit, PreAlert job messages may contain additional information, especially when a security package is being called.

USEREXIT Default Security Exit

The USEREXIT member contains the default security exit included in the basic installation of PreAlert. This exit always sets the return code to zero, allowing access to everything.

When the userdata UDPARMS keyword AUTHXIT=N has been specified, the authorized user IDs must be specified in the UDAUSER macro. If a user ID has not been found, then it will not be authorized.

When AUTHXIT=Y has been specified, all user IDs will be authorized regardless of what has been specified in the UDAUSER macro.

SAMPEXIT Sample Security Exit

The SAMPEXIT member contains code to demonstrate how security may be hard coded into the exit.

In the sample, these rules have been established:

- COMD is available to USERID1 only.
- CMDA is available to USERID1 and USERID2 only.
- IDMS is available to all. USERID3 can monitor IDMSCV1 only.
- Everything else is available to all user IDs.

The sample exit does not check for user signons or authorized user IDs. Therefore, all users would be able to sign on to PreAlert, and the user IDs would be authorized based on the userdata UDAUSER macro, AUTHXIT keyword.

RACFEXIT RACF Security Exit

The RACFEXIT member contains the security exit source code to interface to RACF. When the RACFEXIT is used, the security requests are controlled by RACF for the individual PreAlert users. That is, the security exit will query RACF for the security requests based on the user ID. The RACF security environment is maintained independently (at the TCB level) for each PreAlert user.

Secured line commands and functions are controlled by allowing or denying the user read access to a secured dataset name built by the security exit. The datasets do not actually have to exist; RACF only needs to know that the user has been allowed or denied access to the dataset name.

The security exit builds the secured dataset name based on the four-character line command or function name in the parameter list (PLSTNAME). That name is matched against a table (NAMETBL) that contains the secured names and a class of service for each name. If the secured dataset name is not included in the table, indicating that the function is not secured, the security exit returns to PreAlert with a return code of 0 (zero) allowing access to the line command or function.

When the line command or function name is found in the name table, the exit obtains the matching class of service. The class of service entries (AUTHUSER, AUTHMVS, etc.) are used to group one or more names into a single entry, to build the secured dataset name, and to remember that the entry has been tested already. If that entry has been tested already, the exit returns to PreAlert with the return code based upon the prior test.

To test access to the class of service, the security exit builds the secured dataset name (DSNAME) using the class of service as the last qualifier. The RACHECK macro is issued to check access to the dataset name. If either access is allowed, or the resource (dataset name) is not protected by RACF, the exit returns to PreAlert with a return code of 0 (zero). Otherwise, the exit builds a message and returns to PreAlert with a return code of 8.

User Signons to PreAlert are processed by the security exit through the RACINIT macro to validate the user ID and password and to create the security environment for the user ID. If the RACINIT fails, the security exit selects a message based upon the RACINIT return code, then returns to PreAlert with a return code of 8 (fail with a message).

If the RACINIT was successful, the user ID and password are valid. The security exit then checks to see whether the user is allowed to sign onto PreAlert. The exit uses the MUSR name and AUTHMUSR class of service to test the signon to PreAlert. If the signon is allowed, the exit returns to PreAlert with a return code of 0 (zero). Otherwise, the security exit issues the RACINIT macro to delete the security environment and returns to PreAlert with a return code of 8.

Authorized Users are specified through the userdata UDAUSER macro and AUTHXIT keyword and/or the security exit. If the AUTHXIT=N keyword has been specified for the UDAUSER macro, any user IDs must be specified in the UDAUSER macro in order to be authorized.

If the AUTHXIT=Y keyword has been specified, then a user ID is authorized if specified in the UDAUSER macro or if the security exit allows authority. (The security exit will use the AUTH name and AUTHUSER class of service to allow or deny authority.)

Secured Dataset Names listed in [Figure 20](#) represent the dataset names used by the RACF sample exit. The user must have read access in order to access the associated function(s).

Figure 20 • Secured dataset names

Function	Name	Class	Dataset Name
User signon	MUSR	AUTHMUSR	SYSXXXXX.PREALERT.AUTHMUSR
User	AUTH	AUTHUSER	SYSXXXXX.PREALERT.AUTHUSER
Issue MVS Commands	COMD	AUTHCOMD	SYSXXXXX.PREALERT.AUTHCOMD
.STOPV Command	VSTP		
Memory Zap	MZAP	AUTHMZAP	SYSXXXXX.PREALERT.AUTHMZAP
Monitor APF ListIDMS	IDMS	AUTHIDMS	SYSXXXXX.PREALERT.AUTHIDMS

Modify APF List	APFL	AUTHMVS	SYSXXXXX.PREALERT.AUTHMVS
Cross Memory Dump	CMDA	AUTHMVS	SYSXXXXX.PREALERT.AUTHMVS
Kill an Address Space	KILL	AUTHMVS	SYSXXXXX.PREALERT.AUTHMVS
Reload LPA modules	LPAM	AUTHMVS	SYSXXXXX.PREALERT.AUTHMVS

The sample exit may be modified to include other line commands and classes of service and to build a dataset name more suited to the installation standards.

Secured Line Commands and Functions

The following sections list the normally secured line commands and functions that may be passed to the security exit. The four-character line command or function name will be passed in the name field of the parameter list.

IDMS Interface

All IDMS-related line commands are passed to the exit. If the user has been denied access to the IDMS line command, then they are unable to access any other related line commands. The use of the ICMD, IVRY, and COMD line commands should be controlled since they may be used to alter or cancel IDMS.

Command	Description
IDMS	Monitor an IDMS CV
ICMD	Issue a command to IDMS
IVRY	IDMS Vary command
COMD	Issue MVS command (through IDMS Exception Analysis)

Storage Display and Modification

Storage Display line commands and functions may be included in ["AMVS Security Facility" on page 80](#).

Command	Description
ADDR	Specify virtual storage address for DUMP
CMDA	Specify ASID for cross memory DUMP
DUMH	Memory DUMP header
DUML	Display current DUMP ASID, jobname, and address

Command	Description
DUMP	Memory display
MZAP	Modify memory
KEY0	Allow the user to view non-key-8 fetch-protected storage using the DUMP line command, or to modify non-key-8 storage using the MZAP line command.

Master Console Support

Master Console Support line commands and functions may be included in ["AMVS Security Facility" on page 80](#).

Command	Description
MCON	Master console contents display
COMD	Issue MVS command
RPLY	Outstanding operator reply elements display
MDRM	Display retained messages
MDOM	Delete retained messages

MVS System Services

MVS System Services line commands may be included in the AMVS Security Facility, described on page ["AMVS Security Facility" on page 80](#).

Command	Description
APFL	Modify MVS APF list
KILL	Terminate an address space
LPAM	Load MVS LPA modules
SWPI	Address Space Swap-In
SWPO	Address Space Swap-Out
SWPN	Address Space Swap-In (TRANSWAP)

Dataset Displays

The Dataset Display line commands may be included in the AMVS Security Facility, described in ["AMVS Security Facility" on page 80](#).

Command	Description
DSNA	Datasets allocated to a job (authorized function)

Address Space Restricted Functions

The Address Space Data line commands may be included in ["AMVS Security Facility" on page 80](#).

Command	Description
TCBM	Address Space TCB Map
RGNM	Address Space Region Map
RGNA	Address Space Region Allocation
CDEM	Contents Directory Entry Map
LLEM	Load List Entry Map

Control Commands

The Auto-update and Screen Save functions will be secured only if the SECINT=Y and/or SECSAVE=Y keywords have been specified in the userdata UDPARMS macro.

Command	Description
.INT	Auto-update function
SAVE	Screen Save function

MVS Wait Analysis

The WBGN and all other MVS Wait Analysis line commands will be secured only if the SECWAIT=Y keyword has been specified in the userdata UDPARMS macro.

Command	Description
WBGN	Begin Wait Analysis

Authorized User IDs

The security exit will be called when the user ID has *not* been included in the userdata UDAUSER macro, and the AUTHXIT=Y keyword has been specified in the UDPARMS macro.

Command	Description
AUTH	Authorize the User ID

SMF Logging

The security exit will be called when an authorized user requests statistics logging to the MVS system SMF datasets.

Command	Description
SMFL	Statistics logging to SMF

AMVS Security Facility

Normally, most PreAlert MVS line commands and functions are not secured. The AMVS Security Facility allows either part or all of these to be secured. The AMVS keyword in the userdata UDPARMS macro specifies the areas of PreAlert/MVS to be secured. Refer to ["Userdata Macros" on page 41](#) for more information on these macros.

To use a secured portion of PreAlert MVS, the user must be authorized and have authorization on. Each time PreAlert encounters an AMVS secured line command, AMVS will be used to test the Line Command Exclude feature or the Security Exit is called using AMVS as the line command name. By using AMVS, only one function needs to be tested, as opposed to testing all PreAlert.MVS line commands and functions.

The Line Command Exclude feature userdata UDLCX macro would be coded as:

```
LCXAMVS UDLCX LCX= (AMVS)
```

The security exit parameter list will use AMVS as the function name regardless of the actual line command used.

The parameter list is built as follows:

PARM List	Description
+ 0	AMVS
+ 4	User ID (eight characters)
+ 12	0
+ 16	0

AMVS Secured Functions

The areas of PreAlert MVS that may be secured using the AMVS function are listed below. In some cases, there may be some overlap between normal secured functions and AMVS. If an area or line command is normally secured, the security exit is called using AMVS. The areas overridden by AMVS are underlined.

UDPARMS AMVS Value	Areas Secured
ASID	Address Space Analysis
	Address Space Trace
	Address Space Selection
	<u>Address Space Restricted Functions</u>
DISK	Disk Device Analysis
	Disk Selection Parameters
	Disk Device Trace
TAPE	Tape Statistics
	Tape Selection Parameters
SYST	System Analysis
	System Resources Manager
	Enqueue Contention
	LCU & CHP Utilization
EXA	MVS Exception Analysis
DSN	Dataset Information
	<u>DSNA Line Command</u>

UDPARMS AMVS Value	Areas Secured
DUMP	<u>Storage Display and Modification</u>
MVSS	<u>MVS System Services</u>
MCON	<u>Master Console Support</u>

Index

A

Abend
 Codes 38–39
 Summary 38
Address Space
 Restricted Functions 79, 81
ALTHELP DD 30
ALTHELP File 30
AMVS Security Facility 80
APF
 Authorization 12
 Authorized Libraries 30
Application ID, VTAM 21
ASG-Server Facility 31
Authorization
 Messages 40
 PreAlert 9, 12, 22, 31
 user IDs 12, 70–71, 80
Auto-Start Session
 Restart Limit 26
Auto-start Session 26–27
Auto-update 20, 48

B

Background Session 20, 25, 27

C

CLIST
 CLIST1 31
 CLIST2 31
 CLIST3 17
 CLIST4 21
 PreAlert/TSO ISPF 19
Color Support 20
Console Support, Master 78
Control Commands, PreAlert 79
conventions for this document vi

D

Dataset Displays 79
DD statement 30
Default Security Features 70

E

Event Notification Manager 31
Exception Analysis
 Default Level, IDMS 67
 Default Level, MVS 65
Extended Features 26

I

IDMS
 CV 12
 CV Numbers 66
 Exception Analysis Level Sets 67
 Interface 77
Installation
 PreAlert/Local TSO 31
 PreAlert/TSO 8
 PreAlert/VTAM 21
 Unload JCL 8
 User Data 42
Interface
 PreAlert/TSO ISPF 19
IPL 22
ISPF 20–21
 CLIST 21
 Interface 19
 Menu Panels 20

K

Keyword
 AMVS 50
 AREP 53
 ASFFUN 61
 ASFID 61
 AUTHXIT 22, 49
 CHECK 54
 COMDWTO 51
 EXADATE 59
 EXAPEX 59
 HELPDSN 11, 32, 53
 IADS2 57
 IDMSJCT 57
 IDMSMAX 55

IDMSRCE 55
IDMSSRB 56
IDXDATE 56
IDXPFX 56
IJRNL 56
IJRNLF 56
ILOGINT 57
ILOGSTA 57
ILOGSYN 57
INT 54
ITASKST 57
ITIME 55
IUSMAX 58
LU0SIZE 60
MEMREP 53
MLOGBUF 52
MLOGDSN 11, 51
MLOGDSP 52
MLOGMEM 52
MLOGSMF 51
MTSOID 11, 35, 60
MTSOTIM 60
NOSAVE 54
PAS 17, 30, 35
PIDMS 11, 55
PLOTRED 52
PLOTYEL 52
PRTCLS 51
PRTDEST 51
PRTHOLD 51
RMF 58
SCR 16–17, 23
SCRNLIM 53
SECINT 22, 48
SECSAVE 22, 49
SECWAIT 22, 49
SIRFLME 58
SPFLPA 11, 54
SPYIAT 58
SPYIBF 58
SPYIDB 58
SPYIRU 58
SPYMAS 59
SPYMDD 59
SPYSLM 58
TIDMS 11, 55
TSO 53
UNIT 11, 54
UPW 26
URL 26
USC 26
USR 26
VAP 16, 30
VAPPL 22, 59

VDATA 23, 60
VHOLD 23, 59
VLM 27
VPASS 22, 59
VPS 30
VSNAPC 59
VSNAPH 59
VSWAP 23, 60
VTAM 24
VTAMMAX 23, 59
VTIME 23, 59
VTM 27
WTODSC 51
WTORTC 51

L

LCX 71
Line Command
 .ATH 40
 Exclude Feature 62, 71
 Secured 77
Local TSO
 Using 31
Logon
 PreAlert/TSO 17
 PreAlert/VTAM 24

M

Macros
 UDAUSER 12, 61
 UDCUNUM 10
 UDCVNUM 12, 66
 UDDOM 64
 UDEXAL 65
 UDIDLX 67
 UDLCX 62
 UDPARMS 11, 22
 UDPGN 63
 USERDATA 41
Master Console Support 82
Member
 #MLOGOFF 14–15
 MLOGINIT 14
 MLOGOFFL 14–15
 MLOGPRT1 14–15
 PAPROC 16, 23
Memory Display 77
Menu Panels, ISPF 20
Messages
 Authorization 40
 Started Task 33
Multiple Tasks, PreAlert 30
Multi-Session Software, VTAM 24

- MVS
 - Exception Analysis Level Sets [65](#)
 - Performance Group Names [63](#)
 - System Services [78, 82](#)
- O**
- Operator Commands [28](#)
- P**
- PF key definitions [20](#)
- PreAlert
 - Authorizing [12, 22, 31](#)
 - Local TSO, Using [31](#)
 - TSO [17](#)
 - TSO Installation [8](#)
 - TSO USERDATA [42](#)
 - VTAM [21](#)
- Product Authorization [9](#)
- R**
- RACF [75](#)
- S**
- Secured Functions, Using AMVS [81](#)
- Security
 - AMVS Facility [80](#)
 - Considerations [16, 24, 69](#)
 - Exit [22, 72](#)
 - Exit, Default [75](#)
 - Exit, RACF [75](#)
 - Exit, Sample [74–75](#)
 - Features [70](#)
 - Features, Default [70](#)
- Session
 - Auto-Start [26](#)
 - Background [20, 25](#)
- SHOPMLIB File [30, 32](#)
- Signons, User [70–71, 76](#)
- SMF Logging [80](#)
- Split Screen, ISPF [19](#)
- Started Task Messages [33](#)
- Starting PreAlert [16, 23](#)
- Statistics Logging [14, 80](#)
 - Initialize [14](#)
 - options [51](#)
- Statistics Offload [15](#)
- Statistics Print [15](#)
- Stopping PreAlert [16, 23, 28](#)
- Storage Display and Modification [82](#)
- System Services, MVS [78](#)
- Authorized Program List [31](#)
- U**
- UDPARMS [48](#)
 - Macro Example [42](#)
 - Option Cross-reference [43](#)
 - User Installation Data [42](#)
- UDPARMS Macro Keywords [11](#)
- user IDs, Authorized [12, 61, 70, 80](#)
- USERDATA Options, Specify [10, 22](#)
- V**
- VTAM
 - Application ID [21](#)
 - Multi-session Software [24](#)
- W**
- Wait Analysis, MVS [79](#)
- T**
- TSO

